

# MAXPRO<sup>®</sup> VMS and NVR

Approved Microsoft<sup>®</sup> Windows Patches



---

## Technical Notes

---

# MICROSOFT® WINDOWS PATCHES TESTED WITH MAXPRO®NVR AND MAXPRO®VMS

## Overview

The purpose of this document is to identify the patches that have been delivered by Microsoft® Windows and which have been tested against the current shipping versions of MAXPRO®NVR and MAXPRO®VMS with no adverse effects being observed.

If you have questions concerning the information in this document, please contact Honeywell Technical Support. See the back cover for contact information.

**Windows Patches Tested with MAXPRO®NVR till the Month of:** October, 2019

**Windows Patches Tested with MAXPRO®VMS till the Month of:** October, 2019

**This document contains:**

Section	See...
<ul style="list-style-type: none"><li><i>October - 2019- Microsoft® Windows Patches Tested with MAXPRO®VMS on Windows 2016 Standard and Windows 10 (Enterprise)</i></li><li><i>October - 2019- Microsoft® Windows Patches Tested with MAXPRO®NVR on Windows 7 Embedded</i></li></ul>	<i>page 4</i>
<ul style="list-style-type: none"><li><i>September - 2019- Microsoft® Windows Patches Tested with MAXPRO®VMS on Windows 2016 Standard and Windows 10 (Enterprise)</i></li><li><i>September - 2019- Microsoft® Windows Patches Tested with MAXPRO®NVR on Windows 7 Embedded</i></li></ul>	<i>page 5</i>
<ul style="list-style-type: none"><li><i>August - 2019- Microsoft® Windows Patches Tested with MAXPRO®VMS on Windows 2016 Standard and Windows 10 (Enterprise)</i></li><li><i>August - 2019- Microsoft® Windows Patches Tested with MAXPRO®NVR on Windows 7 Embedded</i></li></ul>	<i>page 6</i>
<ul style="list-style-type: none"><li><i>July - 2019- Microsoft® Windows Patches Tested with MAXPRO®VMS on Windows 2016 Standard and Windows 10 (Enterprise)</i></li><li><i>July - 2019- Microsoft® Windows Patches Tested with MAXPRO®NVR on Windows 7 Embedded</i></li></ul>	<i>page 7</i>
<ul style="list-style-type: none"><li><i>June - 2019- Microsoft® Windows Patches Tested with MAXPRO®VMS on Windows 2012 R2 and Windows 10 (Enterprise)</i></li><li><i>June - 2019- Microsoft® Windows Patches Tested with MAXPRO®NVR on Windows 7 Embedded</i></li></ul>	<i>page 9</i>

Section	See...
<ul style="list-style-type: none"> <li>• <a href="#">May - 2019- Microsoft® Windows Patches Tested with MAXPRO®VMS on Windows 2012 R2 and Windows 10 (Enterprise)</a></li> </ul>	page 7
<ul style="list-style-type: none"> <li>• <a href="#">May - 2019- Microsoft® Windows Patches Tested with MAXPRO®NVR on Windows 7 Embedded</a></li> </ul>	page 9
<ul style="list-style-type: none"> <li>• <a href="#">April - 2019- Microsoft® Windows Patches Tested with MAXPRO®VMS on Windows 2012 R2 and Windows 10 (Enterprise)</a></li> </ul>	page 9
<ul style="list-style-type: none"> <li>• <a href="#">April - 2019- Microsoft® Windows Patches Tested with MAXPRO®NVR on Windows 7 Embedded</a></li> </ul>	page 9
<ul style="list-style-type: none"> <li>• <a href="#">March - 2019- Microsoft® Windows Patches Tested with MAXPRO®VMS on Windows 2012 R2 and Windows 10 (Enterprise)</a></li> </ul>	page 10
<ul style="list-style-type: none"> <li>• <a href="#">March - 2019- Microsoft® Windows Patches Tested with MAXPRO®NVR on Windows 7 Embedded</a></li> </ul>	page 10
<ul style="list-style-type: none"> <li>• <a href="#">February - 2019- Microsoft® Windows Patches Tested with MAXPRO®VMS on Windows 2012 R2 and Windows 10 (Enterprise)</a></li> </ul>	page 10
<ul style="list-style-type: none"> <li>• <a href="#">February - 2019- Microsoft® Windows Patches Tested with MAXPRO®NVR on Windows 7 Embedded</a></li> </ul>	page 11
<ul style="list-style-type: none"> <li>• <a href="#">January - 2019- Microsoft® Windows Patches Tested with MAXPRO®VMS on Windows 2012 R2 and Windows 10 (Enterprise)</a></li> </ul>	page 12
<ul style="list-style-type: none"> <li>• <a href="#">January - 2019- Microsoft® Windows Patches Tested with MAXPRO®NVR on Windows 7 Embedded</a></li> </ul>	page 12
<ul style="list-style-type: none"> <li>• <a href="#">December - 2018- Microsoft® Windows Patches Tested with MAXPRO®VMS on Windows 2012 R2 and Windows 10 (Enterprise)</a></li> </ul>	page 13
<ul style="list-style-type: none"> <li>• <a href="#">December - 2018- Microsoft® Windows Patches Tested with MAXPRO®NVR on Windows 7 Embedded</a></li> </ul>	page 14
<ul style="list-style-type: none"> <li>• <a href="#">November - 2018- Microsoft® Windows Patches Tested with MAXPRO®VMS on Windows 2012 R2 and Windows 10 (Enterprise)</a></li> </ul>	page 14
<ul style="list-style-type: none"> <li>• <a href="#">November - 2018- Microsoft® Windows Patches Tested with MAXPRO®NVR on Windows 7 Embedded</a></li> </ul>	page 14
<ul style="list-style-type: none"> <li>• <a href="#">October - 2018- Microsoft® Windows Patches Tested with MAXPRO®NVR on Windows 7 Embedded</a></li> </ul>	page 14 page 16
<ul style="list-style-type: none"> <li>• <a href="#">September - 2018- Microsoft® Windows Patches Tested with MAXPRO®VMS on Windows 2012 and Windows 10 (Enterprise)</a></li> </ul>	page 16
<ul style="list-style-type: none"> <li>• <a href="#">September - 2018- Microsoft® Windows Patches Tested with MAXPRO®NVR on Windows 7 Embedded</a></li> </ul>	page 16
<ul style="list-style-type: none"> <li>• <a href="#">August - 2018- Microsoft® Windows Patches Tested with MAXPRO®VMS on Windows 2012 and Windows 10 (Enterprise)</a></li> </ul>	page 17
<ul style="list-style-type: none"> <li>• <a href="#">August - 2018- Microsoft® Windows Patches Tested with MAXPRO®NVR on Windows 7 Embedded</a></li> </ul>	page 17
<ul style="list-style-type: none"> <li>• <a href="#">July - 2018- Microsoft® Windows Patches Tested with MAXPRO®VMS on Windows 2012 and Windows 10 (Enterprise)</a></li> </ul>	page 18
<ul style="list-style-type: none"> <li>• <a href="#">July - 2018- Microsoft® Windows Patches Tested with MAXPRO®NVR on Windows 7 Embedded</a></li> </ul>	page 19
<ul style="list-style-type: none"> <li>• <a href="#">June - 2018- Microsoft® Windows Patches Tested with MAXPRO®VMS on Windows 201 and Windows 10 (Enterprise)</a></li> </ul>	page 19
<ul style="list-style-type: none"> <li>• <a href="#">June - 2018- Microsoft® Windows Patches Tested with MAXPRO®NVR on Windows 7 Embedded</a></li> </ul>	page 19

Section	See...
<ul style="list-style-type: none"> <li>• <a href="#">May - 2018- Microsoft® Windows Patches Tested with MAXPRO®VMS on Windows 2012 and Windows 10 (Enterprise)</a></li> <li>• <a href="#">May - 2018- Microsoft® Windows Patches Tested with MAXPRO®NVR on Windows 7 Embedded</a></li> </ul>	<a href="#">page 20</a> <a href="#">page 21</a>
<a href="#">April - 2018- Microsoft® Windows Patches Tested with MAXPRO®VMS/NVR</a>	<a href="#">page 21</a>
<a href="#">March - 2018- Microsoft® Windows Patches Tested with MAXPRO®VMS/NVR</a>	<a href="#">page 22</a>
<a href="#">February - 2018- Microsoft® Windows Patches Tested with MAXPRO®VMS/NVR</a>	<a href="#">page 23</a>
<a href="#">January - 2018- Microsoft® Windows Patches Tested with MAXPRO®VMS/NVR</a>	<a href="#">page 23</a>
<a href="#">2017 -Microsoft® Windows Patches Tested with MAXPRO®VMS/NVR</a>	<a href="#">page 29</a>
<a href="#">December - 2017- Microsoft® Windows Patches Tested with MAXPRO®VMS/NVR</a>	<a href="#">page 24</a>
<a href="#">2016 -Microsoft® Windows Patches Tested with MAXPRO®VMS/NVR</a>	<a href="#">page 31</a>
<b>For MAXPRO®NVR</b>	
<a href="#">2016 - Microsoft® Windows Patches Tested with MAXPRO®NVR</a>	<a href="#">page 31</a>
<a href="#">2015 - Microsoft® Windows Patches Tested with MAXPRO®NVR</a>	<a href="#">page 31</a>
<a href="#">2014- Microsoft® Windows Patches Tested with MAXPRO®NVR</a>	<a href="#">page 31</a>
<a href="#">2013- Microsoft® Windows Patches Tested with MAXPRO®NVR</a>	<a href="#">page 31</a>
<b>For MAXPRO®VMS</b>	
<a href="#">2016 -Windows 7, 32 Bit - Microsoft® Windows Patches Tested with MAXPRO®VMS</a>	<a href="#">page 31</a>
<a href="#">2016 -Windows 7, 64 Bit - Microsoft® Windows Patches Tested with MAXPRO®VMS</a>	<a href="#">page 31</a>
<a href="#">2016 -Windows 8.1, 64/32 Bit - Microsoft® Windows Patches Tested with MAXPRO®VMS</a>	<a href="#">page 31</a>
<a href="#">2016 -Windows 2008, 64Bit - Microsoft® Windows Patches Tested with MAXPRO®VMS</a>	<a href="#">page 60</a>
<a href="#">2016 -Windows 2012 Server R2 - Microsoft® Windows Patches Tested with MAXPRO®VMS</a>	<a href="#">page 67</a>

## MAXPRO® NVR Current Shipping Version

- MAXPRO® NVR (Server and Client) 5.0 Build 509 Rev D + SP1 Patch + SP2 Patch + 5.6 Patch (on Windows 7, 64 bit (Standard) Embedded Image Server + Client)

## MAXPRO® VMS Current Shipping Version

- MAXPRO® VMS Server 500 Build 512 Version + SP1 Patch + SP2 Patch + 5.6 Patch (on Windows Server 2016 Standard 64 bit Server)
- MAXPRO® VMS Client 500 Build 512 Version + SP1 Patch + SP2 Patch + 5.6 Patch (on Windows 10 Pro 64 bit Client)

## MAXPRO® NVR: Windows Patches Tested with Microsoft® Windows OS

- Microsoft® Windows Embedded Standard 7 SP1, 32-bit / 64-bit (Server + Client)

## MAXPRO® VMS: Windows Patches Tested with Microsoft® Windows OS

- Microsoft® Windows 10 Enterprise, 32-bit / 64-bit Client.
- Microsoft Windows 2016 Standard 64 bit Server

## October - 2019- Microsoft® Windows Patches Tested with MAXPRO® VMS on Windows 2016 Standard and Windows 10 (Enterprise)

Microsoft Knowledge Base Article ID	Description
<a href="#">KB4521858</a>	Servicing stack update for Windows 10 version 1607: October 8, 2019
<a href="#">KB4515871</a>	KB4515871 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 version 1903 and Windows 10 version 1909
<a href="#">KB4521863</a>	Servicing stack update for Windows 10 version 1903: October 8, 2019
<a href="#">KB4517389</a>	October 8, 2019—KB4517389 (OS Build 18362.418)

## October - 2019- Microsoft® Windows Patches Tested with MAXPRO® NVR on Windows 7 Embedded

Microsoft Knowledge Base Article ID	Description
<a href="#">KB4519976</a>	October 8, 2019—KB4519976 (Monthly Rollup)

## September - 2019- Microsoft® Windows Patches Tested with MAXPRO® VMS on Windows 2016 Standard and Windows 10 (Enterprise)

Microsoft Knowledge Base Article ID	Description
<a href="#">KB4512574</a>	Servicing stack update for Windows 10 version 1607: September 10, 2019
<a href="#">KB4507459</a>	KB4507459 (OS Build 14393.3115)
<a href="#">KB4514359</a>	September 10, 2019-KB4514359 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 version 1903 and Windows 10 version 1909
<a href="#">KB4515383</a>	Servicing stack update for Windows 10 version 1903: September 10, 2019
<a href="#">KB4516115</a>	Security Update for Adobe Flash Player: September 10, 2019
<a href="#">KB4515384</a>	September 10, 2019—KB4515384 (OS Build 18362.356)

## September - 2019- Microsoft® Windows Patches Tested with MAXPRO® NVR on Windows 7 Embedded

Microsoft Knowledge Base Article ID	Description
<a href="#">KB4474419</a>	SHA-2 code signing support update for Windows Server 2008 R2, Windows 7, and Windows Server 2008: September 23, 2019
<a href="#">KB4516655</a>	Servicing stack update for Windows 7 SP1 and Server 2008 R2 SP1: September 10, 2019
<a href="#">KB4516065</a>	September 10, 2019—KB4516065 (Monthly Rollup)

## August - 2019- Microsoft® Windows Patches Tested with MAXPRO® VMS on Windows 2016 Standard and Windows 10 (Enterprise)

Microsoft Knowledge Base Article ID	Description
<a href="#">KB4506991</a>	KB4506991 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10, version 1903

<b>Microsoft Knowledge Base Article ID</b>	<b>Description</b>
<a href="#">KB4503308</a>	Security Update for Adobe Flash Player
<a href="#">KB4515530</a>	Servicing stack update for Windows 10 version 1903: August 27, 2019
<a href="#">KB4512508</a>	August 13, 2019—KB4512508 (OS Build 18362.295)

## August - 2019- Microsoft® Windows Patches Tested with MAXPRO® NVR on Windows 7 Embedded

<b>Microsoft Knowledge Base Article ID</b>	<b>Description</b>
<a href="#">KB4344152</a>	Description of the Security and Quality Rollup for .NET Framework 3.5.1 for Windows 7 SP1 and Windows Server 2008 R2 SP1 (KB 4344152)
<a href="#">KB4474419</a>	SHA-2 code signing support update for Windows Server 2008 R2, Windows 7, and Windows Server 2008: August 13, 2019
<a href="#">KB4512506</a>	August 13, 2019—KB4512506 (Monthly Rollup)

## July - 2019- Microsoft® Windows Patches Tested with MAXPRO® VMS on Windows 2016 Standard and Windows 10 (Enterprise)

<b>Microsoft Knowledge Base Article ID</b>	<b>Description</b>
<a href="#">KB4509091</a>	Servicing stack update for Windows 10, Version 1607: July 9, 2019
<a href="#">KB4507460</a>	July 9, 2019—KB4507460 (OS Build 14393.3085)
<a href="#">KB4509094</a>	Servicing stack update for Windows 10, Version 1803: July 9, 2019

## July - 2019- Microsoft® Windows Patches Tested with MAXPRO® NVR on Windows 7 Embedded

<a href="#">Microsoft Knowledge Base Article ID</a>	Description
<a href="#">KB4507004</a>	Security and Quality Rollup for .NET Framework 3.5.1 for Windows 7 SP1 and Server 2008 R2 SP1 and Server 2008 (KB4507004)
<a href="#">KB4507449</a>	July 9, 2019—KB4507449 (Monthly Rollup)

## June - 2019- Microsoft® Windows Patches Tested with MAXPRO® VMS on Windows 2012 R2 and Windows 10 (Enterprise)

<a href="#">Microsoft Knowledge Base Article ID</a>	Description
<a href="#">KB4497398</a>	Servicing stack update for Windows 10, Version 1803
<a href="#">KB4503308</a>	Security Update for Adobe Flash Player: June 11, 2019
<a href="#">KB4503288</a>	June 18, 2019—KB4503288 (OS Build 17134.858)

## June - 2019- Microsoft® Windows Patches Tested with MAXPRO® NVR on Windows 7 Embedded

<a href="#">Microsoft Knowledge Base Article ID</a>	Description
<a href="#">KB4499175</a>	KB4499175 (Security-only update)
<a href="#">KB4503292</a>	June 11, 2019—KB4503292 (Monthly Rollup)

## May - 2019- Microsoft® Windows Patches Tested with MAXPRO® VMS on Windows 2012 R2 and Windows 10 (Enterprise)



<b>Microsoft Knowledge Base Article ID</b>	<b>Description</b>
<a href="#">KB4495585</a>	Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1, RT 8.1, and Server 2012 R2 (KB4495585)
<a href="#">KB4495608</a>	Security and Quality Rollup for .NET Framework 3.5 for Windows 8.1, RT 8.1, and Server 2012 R2 (KB4495608)
<a href="#">KB4497932</a>	Security Update for Adobe Flash Player: May 14, 2019
<a href="#">KB4505050</a>	Cumulative update for Internet Explorer: May 18, 2019
<a href="#">KB4499182</a>	May 23, 2019—KB4499182 (Preview of Monthly Rollup)

## May - 2019- Microsoft® Windows Patches Tested with MAXPRO® NVR on Windows 7 Embedded

<a href="#">Microsoft Knowledge Base Article ID</a>	Description
<a href="#">KB4495606</a>	Security and Quality Rollup for .NET Framework 3.5.1 for Windows 7 SP1 and Server 2008 R2 SP1 (KB4495606)
<a href="#">KB4505050</a>	Cumulative update for Internet Explorer: May 18, 2019
<a href="#">KB4499164</a>	May 14, 2019—KB4499164 (Monthly Rollup)

## April - 2019- Microsoft® Windows Patches Tested with MAXPRO® VMS on Windows 2012 R2 and Windows 10 (Enterprise)

<a href="#">Microsoft Knowledge Base Article ID</a>	Description
<a href="#">KB4486459</a>	DST changes in Windows for Chile
<a href="#">KB4488663</a>	Description of the Update for .NET Framework 3.5 for Windows 8.1 and Server 2012 R2 (KB 4488663)
<a href="#">KB4488665</a>	Description of the Update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, and 4.7.2 for Windows 8.1, RT 8.1 and Server 2012 R2 (KB 4488665)
<a href="#">KB4490128</a>	Time zone changes in Windows for São Tomé and Príncipe, and Qyzylorda
<a href="#">KB4493478</a>	Security Update for Adobe Flash Player: April 9, 2019
<a href="#">KB4493443</a>	April 25, 2019—KB4493443 (Preview of Monthly Rollup)
<a href="#">KB4346084</a>	KB4346084: Intel microcode updates
<a href="#">KB4493464</a>	April 9, 2019—KB4493464 (OS Build 17134.706)

## April - 2019- Microsoft® Windows Patches Tested with MAXPRO® NVR on Windows 7 Embedded

<a href="#">Microsoft Knowledge Base Article ID</a>	Description
<a href="#">KB4488662</a>	Description of the Update for .NET Framework 3.5.1 for Windows 7 SP1 and Server 2008 R2 SP1 (KB 4488662)
<a href="#">KB4493472</a>	April 9, 2019—KB4493472 (Monthly Rollup)

## March - 2019- Microsoft® Windows Patches Tested with MAXPRO® VMS on Windows 2012 R2 and Windows 10 (Enterprise)

Microsoft Knowledge Base Article ID	Description
<a href="#">KB4489907</a>	Security Update for Adobe Flash Player: March 12, 2019
<a href="#">KB4489893</a>	March 19, 2019—KB4489893 (Preview of Monthly Rollup)

## March - 2019- Microsoft® Windows Patches Tested with MAXPRO® NVR on Windows 7 Embedded

Microsoft Knowledge Base Article ID	Description
<a href="#">KB4474419</a>	SHA-2 code signing support update for Windows Server 2008 R2 and Windows 7: March 12, 2019
<a href="#">KB4490628</a>	Servicing stack update for Windows 7 SP1 and Windows Server 2008 R2 SP1: March 12, 2019
<a href="#">KB4489878</a>	March 12, 2019—KB4489878 (Monthly Rollup)

## February - 2019- Microsoft® Windows Patches Tested with MAXPRO® VMS on Windows 2012 R2 and Windows 10 (Enterprise)

Microsoft Knowledge Base Article ID	Description
<a href="#">KB4483450</a>	Description of the Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, and 4.7.2 for Windows 8.1, RT 8.1, and Server 2012 R2 (KB 4483450)
<a href="#">KB4483459</a>	Description of the Security and Quality Rollup for .NET Framework 3.5 for Windows 8.1, RT 8.1, and Server 2012 R2 (KB 4483459)
<a href="#">KB4486545</a>	Description of Preview of Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, and 4.7.2 for Windows 8.1, Windows 8.1 RT and Server 2012 R2 (KB4486545)
<a href="#">KB4487038</a>	Security Update for Adobe Flash Player: February 12, 2019
<a href="#">KB4487016</a>	February 19, 2019—KB4487016 (Preview of Monthly Rollup)
<a href="#">KB4346084</a>	KB4346084: Intel microcode updates

Microsoft Knowledge Base Article ID	Description
<a href="#">KB4485449</a>	Servicing stack update for Windows Server version 1803 and Windows 10 version 1803: February 12, 2019
<a href="#">KB4487038</a>	Security Update for Adobe Flash Player: February 12, 2019
<a href="#">KB4487029</a>	February 19, 2019—KB4487029 (OS Build 17134.619)

## February - 2019- Microsoft® Windows Patches Tested with MAXPRO® NVR on Windows 7 Embedded

Microsoft Knowledge Base Article ID	Description
<a href="#">KB4483458</a>	Description of the Security and Quality Rollup for .NET Framework 3.5.1 for Windows 7 SP1 and Server 2008 R2 SP1 (KB 4483458)
<a href="#">KB4486563</a>	February 12, 2019—KB4486563 (Monthly Rollup)
<a href="#">KB4074598</a>	February 13, 2018—KB4074598 (Monthly Rollup)

## January - 2019- Microsoft® Windows Patches Tested with MAXPRO® VMS on Windows 2012 R2 and Windows 10 (Enterprise)

Microsoft Knowledge Base Article ID	Description
<a href="#">KB4345424</a>	Improvements and fixes - Windows 8.1 and Server 2012 R2
<a href="#">KB4480054</a>	Description of the Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, and 4.7.2 for Windows 8.1, RT 8.1, and Server 2012 R2 (KB 4480054)
<a href="#">KB4480064</a>	Description of the Security and Quality Rollup for .NET Framework 3.5 for Windows 8.1, RT 8.1, and Server 2012 R2 (KB 4480064)
<a href="#">KB4480071</a>	Description of the Security Only update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, and 4.7.2 for Windows 8.1 and Server 2012 R2 (KB 4480071)
<a href="#">KB4480086</a>	Description of the Security Only update for .NET Framework 3.5 for Windows 8.1 and Server 2012 R2 (KB 4480086)
<a href="#">KB4480095</a>	Description of Preview of Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, and 4.7.2 for Windows 8.1, RT 8.1, and Server 2012 R2 (KB 4480095)
<a href="#">KB4480964</a>	January 8, 2019—KB4480964 (Security-only update)
<a href="#">KB4480965</a>	Cumulative security update for Internet Explorer: January 8, 2019
<a href="#">KB4480979</a>	Security update for Adobe Flash Player: January 8, 2019
<a href="#">KB4480969</a>	January 15, 2019—KB4480969 (Preview of Monthly Rollup)
<a href="#">KB4100347</a>	KB4100347: Intel microcode updates
<a href="#">KB4480979</a>	Security update for Adobe Flash Player: January 8, 2019
<a href="#">KB4480966</a>	January 8, 2019—KB4480966 (OS Build 17134.523)

## January - 2019- Microsoft® Windows Patches Tested with MAXPRO® NVR on Windows 7 Embedded

Microsoft Knowledge Base Article ID	Description
<a href="#">KB4099950</a>	NIC settings are replaced or static IP address settings are lost after you install KB4088875 or KB4088878
<a href="#">KB4480063</a>	Description of the Security and Quality Rollup for .NET Framework 3.5.1 for Windows 7 SP1 and Server 2008 R2 SP1 (KB 4480063)
<a href="#">KB4480085</a>	Description of the Security Only update for .NET Framework 3.5.1 for Windows 7 SP1 and Server 2008 R2 SP1 (KB 4480085)

<b>Microsoft Knowledge Base Article ID</b>	<b>Description</b>
<a href="#">KB4480960</a>	January 8, 2019—KB4480960 (Security-only update)
<a href="#">KB4480965</a>	Cumulative security update for Internet Explorer: January 8, 2019
<a href="#">KB4480970</a>	January 8, 2019—KB4480970 (Monthly Rollup)

## 2018 -Microsoft® Windows Patches Tested with MAXPRO®VMS/NVR

### December - 2018- Microsoft® Windows Patches Tested with MAXPRO®VMS on Windows 2012 R2 and Windows 10 (Enterprise)

<b>Microsoft Knowledge Base Article ID</b>	<b>Description</b>
<a href="#">KB4468323</a>	DST and time zone changes in Windows for Morocco and Volgograd
<a href="#">KB4470199</a>	Cumulative security update for Internet Explorer: December 11, 2018
<a href="#">KB4470499</a>	Description of the Security Only update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, and 4.7.2 for Windows 8.1 and Server 2012 R2 (KB 4470499)
<a href="#">KB4470602</a>	Description of the Security Only update for .NET Framework 3.5 for Windows 8.1 and Server 2012 R2 (KB 4470602)
<a href="#">KB4470630</a>	Description of the Security and Quality Rollup for .NET Framework 3.5 for Windows 8.1, RT 8.1, and Server 2012 R2 (KB 4470630)
<a href="#">KB4470639</a>	Description of the Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, and 4.7.2 for Windows 8.1, RT 8.1, and Server 2012 R2 (KB 4470639)
<a href="#">KB4471322</a>	December 11, 2018—KB4471322 (Security-only update)
<a href="#">KB4471331</a>	Security update for Adobe Flash Player: December 5, 2018
<a href="#">KB4483187</a>	Cumulative security update for Internet Explorer: December 19, 2018
<a href="#">KB4471320</a>	December 11, 2018—KB4471320 (Monthly Rollup)
<a href="#">KB4477137</a>	Servicing stack update for Windows Server, version 1803 and Windows 10, version 1803: December 11, 2018
<a href="#">KB4483541</a>	Update for Unified Update Platform (UUP): December 20, 2018
<a href="#">KB4471324</a>	December 11, 2018—KB4471324 (OS Build 17134.471)
<a href="#">KB4483234</a>	December 19, 2018—KB4483234 (OS Build 17134.472)

## December - 2018- Microsoft® Windows Patches Tested with MAXPRO® NVR on Windows 7 Embedded

Microsoft Knowledge Base Article ID	Description
<a href="#">KB4468323</a>	DST and time zone changes in Windows for Morocco and Volgograd
<a href="#">KB4470199</a>	Cumulative security update for Internet Explorer: December 11, 2018
<a href="#">KB4470600</a>	Description of the Security Only update for .NET Framework 3.5.1 for Windows 7 SP1 and Server 2008 R2 SP1 (KB 4470600)
<a href="#">KB4470641</a>	Description of the Security and Quality Rollup for .NET Framework 3.5 for Windows 7 SP1 and Server 2008 R2 SP1 (KB 4470641)
<a href="#">KB4471328</a>	December 11, 2018—KB4471328 (Security-only update)
<a href="#">KB4483187</a>	Cumulative security update for Internet Explorer: December 19, 2018
<a href="#">KB2533552</a>	An update that prevents a "0xC0000034" error message when you try to install Windows 7 SP1, Windows Server 2008 R2 SP1, or Windows Embedded Standard 7 SP1 is available
<a href="#">KB976932</a>	Information about Service Pack 1 for Windows 7 and for Windows Server 2008 R2
<a href="#">KB4471318</a>	December 11, 2018—KB4471318 (Monthly Rollup)

## November - 2018- Microsoft® Windows Patches Tested with MAXPRO® VMS on Windows 2012 R2 and Windows 10 (Enterprise)

Microsoft Knowledge Base Article ID	Description
<a href="#">KB4467703</a>	November 13, 2018—KB4467703 (Security-only update)
<a href="#">KB4477029</a>	Security update for Adobe Flash Player: November 20, 2018
<a href="#">KB4467697</a>	November 13, 2018—KB4467697 (Monthly Rollup)
<a href="#">KB4465663</a>	Servicing stack update for Windows Server, version 1803 and Windows 10, version 1803: November 13, 2018
<a href="#">KB4467694</a>	Security update for Adobe Flash Player: November 13, 2018
<a href="#">KB4477029</a>	Security update for Adobe Flash Player: November 20, 2018
<a href="#">KB4467702</a>	November 13, 2018—KB4467702 (OS Build 17134.407)

## November - 2018- Microsoft® Windows Patches Tested with MAXPRO® NVR on Windows 7 Embedded

<b>Microsoft Knowledge Base Article ID</b>	<b>Description</b>
<a href="#">KB4339284</a>	Time zone and DST changes in Windows for North Korea
<a href="#">KB4467106</a>	November 13, 2018—KB4467106 (Security-only update)
<a href="#">KB958488</a>	An update is available for Microsoft .NET Framework 3.5 Service Pack 1 on Windows 7 and Windows Server 2008 R2
<a href="#">KB4467107</a>	November 13, 2018—KB4467107 (Monthly Rollup)

## October - 2018- Microsoft® Windows Patches Tested with MAXPRO® VMS on Windows 2012 R2 and Windows 10 (Enterprise)

<b>Microsoft Knowledge Base Article ID</b>	<b>Description</b>
<a href="#">KB4459935</a>	Description of Preview of Quality Rollup for .NET Framework 3.5 for Windows 8.1 and Server 2012 R2 (KB 4459935)
<a href="#">KB4459941</a>	Description of Preview of Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, and 4.7.2 for Windows 8.1, RT 8.1, and Server 2012 R2 (KB 4459941)
<a href="#">KB4462930</a>	Update for Adobe Flash Player: October 9, 2018
<a href="#">KB4462921</a>	October 18, 2018—KB4462921 (Preview of Monthly Rollup)
<a href="#">KB4462933</a>	October 24, 2018—KB4462933 (OS Build 17134.376)



## October - 2018- Microsoft® Windows Patches Tested with MAXPRO® NVR on Windows 7 Embedded

<b>Microsoft Knowledge Base Article ID</b>	<b>Description</b>
<a href="#">KB4459934</a>	Description of Preview of Quality Rollup for .NET Framework 3.5.1 for Windows 7 SP1 and Windows Server 2008 R2 SP1 (KB 4459934)
<a href="#">KB4462923</a>	October 9, 2018—KB4462923 (Monthly Rollup)

## September - 2018- Microsoft® Windows Patches Tested with MAXPRO® VMS on Windows 2012 and Windows 10 (Enterprise)

<b>Microsoft Knowledge Base Article ID</b>	<b>Description</b>
<a href="#">KB4457009</a>	Description of Preview of Quality Rollup for .NET Framework 3.5 for Windows 8.1, RT 8.1, and Server 2012 R2 (KB 4457009)
<a href="#">KB4457015</a>	Description of Preview of Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, and 4.7.2 for Windows 8.1, RT 8.1, and Server 2012 R2 (KB 4457015)
<a href="#">KB4457034</a>	Description of the Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, and 4.7.2 for Windows 8.1, RT 8.1 and Server 2012 R2 (KB 4457034)
<a href="#">KB4457045</a>	Description of the Security and Quality Rollup for .NET Framework 3.5 for Windows 8.1 and Server 2012 R2 (KB 4457045)
<a href="#">KB4457146</a>	Security update for Adobe Flash Player: September 11, 2018
<a href="#">KB4457133</a>	September 20, 2018—KB4457133 (Preview of Monthly Rollup)
<a href="#">KB4100347</a>	KB4100347: Intel microcode updates
<a href="#">KB4458469</a>	September 26, 2018—KB4458469 (OS Build 17134.320)

## September - 2018- Microsoft® Windows Patches Tested with MAXPRO® NVR on Windows 7 Embedded

<b>Microsoft Knowledge Base Article ID</b>	<b>Description</b>
<a href="#">KB4457008</a>	Description of Preview of Quality Rollup for .NET Framework 3.5.1 for Windows 7 SP1 and Server 2008 R2 SP1 (KB 4457008)
<a href="#">KB4457044</a>	Description of the Security and Quality Rollup for .NET Framework 3.5.1 for Windows 7 SP1 and Server 2008 R2 SP1 (KB 4457044)
<a href="#">KB4457144</a>	September 11, 2018—KB4457144 (Monthly Rollup)

## August - 2018- Microsoft® Windows Patches Tested with MAXPRO® VMS on Windows 2012 and Windows 10 (Enterprise)

<b>Microsoft Knowledge Base Article ID</b>	<b>Description</b>
<a href="#">KB4343902</a>	Security update for Adobe Flash Player: August 14, 2018
<a href="#">KB4344145</a>	Description of the Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, and 4.7.2 for Windows 8.1, RT 8.1, and Server 2012 R2 (KB 4344145)
<a href="#">KB4344153</a>	Description of the Security and Quality Rollup for .NET Framework 3.5 for Windows 8.1, RT 8.1, and Server 2012 R2 (KB 4344153)
<a href="#">KB4343898</a>	August 14, 2018—KB4343898 (Monthly Rollup)
<a href="#">KB4100347</a>	KB4100347: Intel microcode updates
<a href="#">KB4287903</a>	Security update for Adobe Flash Player
<a href="#">KB4343669</a>	Servicing stack update for Windows 10, version 1803
<a href="#">KB4343902</a>	Security update for Adobe Flash Player: August 14, 2018
<a href="#">KB4343909</a>	August 14, 2018—KB4343909 (OS Build 17134.228)

## August - 2018- Microsoft® Windows Patches Tested with MAXPRO® NVR on Windows 7 Embedded

Microsoft Knowledge Base Article ID	Description
<a href="#">KB4344152</a>	Description of the Security and Quality Rollup for .NET Framework 3.5.1 for Windows 7 SP1 and Windows Server 2008 R2 SP1 (KB 4344152)
<a href="#">KB4343900</a>	August 14, 2018—KB4343900 (Monthly Rollup)

## July - 2018- Microsoft® Windows Patches Tested with MAXPRO® VMS on Windows 2012 and Windows 10 (Enterprise)

Microsoft Knowledge Base Article ID	Description
<a href="#">KB4284878</a>	KB4284878 (Security-only update)
<a href="#">KB4338415</a>	Description of the Security and Quality Rollup updates for .NET Framework 4.5.2 for Windows 8.1, RT 8.1, and Server 2012 R2 (KB 4338415)
<a href="#">KB4338424</a>	Description of the Security and Quality Rollup updates for .NET Framework 3.5 SP1 for Windows 8.1, RT 8.1, and Server 2012 R2 (KB 4338424)
<a href="#">KB4338600</a>	Description of the Security Only update for .NET Framework 4.5.2 for Windows 8.1 and Server 2012 R2 (KB 4338600)
<a href="#">KB4338605</a>	Description of the Security Only update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1 and 4.7.2 for Windows 8.1 and Server 2012 R2 (KB 4338605)
<a href="#">KB4338613</a>	Description of the Security Only update for .NET Framework 3.5 SP1 for Windows 8.1 and Server 2012 R2 (KB 4338613)
<a href="#">KB4338824</a>	July 10, 2018—KB4338824 (Security-only update)
<a href="#">KB4338832</a>	Security update for Adobe Flash Player: July 10, 2018
<a href="#">KB4338815</a>	July 10, 2018—KB4338815 (Monthly Rollup)
<a href="#">KB4287903</a>	Security update for Adobe Flash Player
<a href="#">KB4338832</a>	Security update for Adobe Flash Player: July 10, 2018
<a href="#">KB4339420</a>	Servicing stack update for Windows 10, version 1709: July 10, 2018
<a href="#">KB4338825</a>	<a href="http://support.microsoft.com/?kbid=4338825">http://support.microsoft.com/?kbid=4338825</a>

## July - 2018- Microsoft® Windows Patches Tested with MAXPRO® NVR on Windows 7 Embedded

<b>Microsoft Knowledge Base Article ID</b>	<b>Description</b>
<a href="#">KB4338423</a>	Description of the Security and Quality Rollup updates for .NET Framework 3.5.1 for Windows 7 SP1 and Server 2008 R2 SP1 (KB 4338423)
<a href="#">KB4338612</a>	Description of the Security Only update for .NET Framework 3.5.1 for Windows 7 SP1 and Server 2008 R2 SP1 (KB 4338612)
<a href="#">KB4338823</a>	July 10, 2018—KB4338823 (Security-only update)
<a href="#">KB4338818</a>	July 10, 2018—KB4338818 (Monthly Rollup)

## June - 2018- Microsoft® Windows Patches Tested with MAXPRO® VMS on Windows 201 and Windows 10 (Enterprise)

<b>Microsoft Knowledge Base Article ID</b>	<b>Description</b>
<a href="#">KB4291497</a>	June 2018 Preview of the Quality Rollups for .NET Framework 3.5, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, and 4.7.1 for Windows 8.1, RT 8.1, and Server 2012 R2 (KB 4291497)
<a href="#">KB4284863</a>	June 21, 2018—KB4284863 (Preview of Monthly Rollup)
<a href="#">KB4284815</a>	June 12, 2018—KB4284815 (Monthly Rollup)
<a href="#">KB890830</a>	Remove specific prevalent malware with Windows Malicious Software Removal Tool
<a href="#">KB4287903</a>	Security update for Adobe Flash Player: June 7, 2018
<a href="#">KB4284822</a>	June 21, 2018—KB4284822 (OS Build 16299.522)

## June - 2018- Microsoft® Windows Patches Tested with MAXPRO® NVR on Windows 7 Embedded

<b>Microsoft Knowledge Base Article ID</b>	<b>Description</b>
<a href="#">KB4291493</a>	June 2018 Preview of the Quality Rollups for .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, and 4.7.1 for Windows 7 SP1 and Server 2008 R2 SP1 (KB 4291493)
<a href="#">KB4284826</a>	June 12, 2018—KB4284826 (Monthly Rollup)

## May - 2018- Microsoft® Windows Patches Tested with MAXPRO® VMS on Windows 2012 and Windows 10 (Enterprise)

<b>Microsoft Knowledge Base Article ID</b>	<b>Description</b>
<a href="#">KB4095515</a>	Description of the Security Only update for .NET Framework 3.5 SP1 for Windows 8.1 and Server 2012 R2 (KB 4095515)
<a href="#">KB4095875</a>	Description of the Security and Quality Rollup for .NET Framework 3.5 for Windows 8.1 and Server 2012 R2 (KB 4095875)
<a href="#">KB4096236</a>	Description of the Security Only update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7 and 4.7.1 for Windows 8.1, RT 8.1 and Server 2012 R2 (KB 4096236)
<a href="#">KB4096417</a>	Description of the Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, and 4.7.1 for Windows 8.1, RT 8.1, and Server 2012 R2 (KB 4096417)
<a href="#">KB4098972</a>	Description of Preview of Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7 and 4.7.1 for Windows 8.1, RT 8.1 and Server 2012 R2 (KB 4098972)
<a href="#">KB4103715</a>	May 8, 2018—KB4103715 (Security-only update)
<a href="#">KB4103729</a>	Security update for Adobe Flash Player: May 8, 2018
<a href="#">KB4103768</a>	Cumulative security update for Internet Explorer: May 08, 2018
<a href="#">KB4130978</a>	Time zone and DST changes in Windows for Morocco and the West Bank and Gaza
<a href="#">KB4103724</a>	May 17, 2018—KB4103724 (Preview of Monthly Rollup)
<a href="#">KB4090007</a>	KB4090007: Intel microcode updates
<a href="#">KB4131372</a>	Servicing stack update for Windows 10 Version 1709: May 8, 2018
<a href="#">KB4132650</a>	Servicing stack update for Windows 10 Version 1709: May 21, 2018
<a href="#">KB4103714</a>	May 21, 2018—KB4103714 (OS Build 16299.461)

## May - 2018- Microsoft® Windows Patches Tested with MAXPRO® NVR on Windows 7 Embedded

<b>Microsoft Knowledge Base Article ID</b>	<b>Description</b>
<a href="#">KB4095514</a>	Description of the Security Only update for .NET Framework 3.5.1 for Windows 7 SP1 and Server 2008 R2 SP1 (KB 4095514)
<a href="#">KB4095874</a>	Description of the Security and Quality Rollup for .NET Framework 3.5.1 for Windows 7 SP1 and Server 2008 R2 SP1 (KB 4095874)
<a href="#">KB4103712</a>	May 8, 2018—KB4103712 (Security-only update)
<a href="#">KB4103768</a>	Cumulative security update for Internet Explorer: May 08, 2018
<a href="#">KB4103718</a>	May 8, 2018—KB4103718 (Monthly Rollup)

## April - 2018- Microsoft® Windows Patches Tested with MAXPRO® VMS/NVR

<b>Microsoft Knowledge Base Article ID</b>	<b>Description</b>
<a href="#">KB4092946</a>	Cumulative security update for Internet Explorer: April 10, 2018
<a href="#">KB4093110</a>	Security update for Adobe Flash Player: April 10, 2018
<a href="#">KB4093115</a>	April 10, 2018—KB4093115 (Security-only update)
<a href="#">KB4093121</a>	April 17, 2018—KB4093121 (Preview of Monthly Rollup)
<a href="#">KB4093108</a>	April 10, 2018—KB4093108 (Security-only update)
<a href="#">KB4096040</a>	Cumulative security update for Internet Explorer
<a href="#">KB4100480</a>	Windows kernel update for CVE-2018-1038
<a href="#">KB4093118</a>	April 10, 2018—KB4093118 (Monthly Rollup)
<a href="#">KB4090007</a>	Intel microcode updates
<a href="#">KB4099989</a>	Servicing stack update for Windows 10, version 1709: April 10, 2018
<a href="#">KB4093112</a>	April 10, 2018—KB4093112 (OS Build 16299.371)

# March - 2018- Microsoft® Windows Patches Tested with MAXPRO® VMS/NVR

<b>Microsoft Knowledge Base Article ID</b>	<b>Description</b>
<a href="#">KB4074598</a>	February 13, 2018—KB4074598 (Monthly Rollup). This security update includes improvements and fixes that were a part of update KB4057400 (released January 19, 2018)
<a href="#">KB4074597</a>	This security update includes quality improvements. No new operating system features are being introduced in this update.
<a href="#">KB4074736</a>	Cumulative security update for Internet Explorer
<a href="#">KB4077561</a>	Stop errors caused by spurious interrupt on systems PIC and APIC interrupt controllers
<a href="#">KB4088785</a>	Security update for Adobe Flash Player: March 13, 2018
<a href="#">KB4088876</a>	March 13, 2018—KB4088876 (Monthly Rollup)
<a href="#">KB4090007</a>	KB4090007: Intel microcode updates
<a href="#">KB4090914</a>	Servicing stack update for Windows 10 Version 1709: March 5, 2018
<a href="#">KB4088776</a>	March 13, 2018—KB4088776 (OS Build 16299.309)

## February - 2018- Microsoft® Windows Patches Tested with MAXPRO® VMS/NVR

Microsoft Knowledge Base Article ID	Description
<a href="#">KB4074598</a>	This security update includes improvements and fixes that were a part of update KB4057400 (released January 19, 2018)
<a href="#">KB4074587</a>	This security update includes quality improvements. No new operating system features are being introduced in this update.
<a href="#">KB4054998</a>	Description of Security and Quality Rollup for .NET Framework 3.5.1 for Windows 7 SP1 and Server 2008 R2 SP1 (KB 4054998)
<a href="#">KB4074736</a>	Cumulative security update for Internet Explorer: February 13, 2018
<a href="#">KB4058258</a>	This update includes quality improvements. No new operating system features are being introduced in this update.
<a href="#">KB4074588</a>	This update includes quality improvements. No new operating system features are being introduced in this update.
<a href="#">KB4074595</a>	Security update for Adobe Flash Player: February 6, 2018
<a href="#">KB4087256</a>	Servicing stack update for Windows 10 Version 1709, February 13, 2018
<a href="#">KB4058702</a>	Servicing stack update for Windows 10 Version 1709
<a href="#">KB4054999</a>	Description of Security and Quality Rollup for .NET Framework 3.5 SP1 for Windows 8.1, RT 8.1, and Server 2012 R2 (KB 4054999)
<a href="#">KB4057401</a>	This non-security update includes improvements and fixes that were a part of KB4056895 (released January 8, 2018) and also includes new quality improvements as a preview of the next Monthly Rollup update
<a href="#">KB4077561</a>	Stop errors caused by spurious interrupt on systems PIC and APIC interrupt controllers
<a href="#">KB890830</a>	Remove specific prevalent malware with Windows Malicious Software Removal Tool

## January - 2018- Microsoft® Windows Patches Tested with MAXPRO® VMS/NVR

Microsoft Knowledge Base Article ID	Description
<a href="#">KB4054854</a>	.NET Framework 4.7.1 Update for Windows 8.1, Windows Server 2012 R2 and Windows RT 8.1 (KB4054854)
<a href="#">KB4056887</a>	Security update for Adobe Flash Player: January 9, 2018
<a href="#">KB4056898</a>	January 3, 2018—KB4056898 (Security-only update) Applies to: Windows 8.1, Windows Server 2012 R2 Standard



Microsoft Knowledge Base Article ID	Description
<a href="#">KB4054519</a>	December 12, 2017—KB4054519 (Monthly Rollup)
<a href="#">KB4051956</a>	Time zone and DST changes in Windows for Northern Cyprus, Sudan, and Tonga
<a href="#">KB4054176</a>	Description of the Security Only update for .NET Framework 3.5.1 for Windows 7 SP1 and Windows Server 2008 R2 SP1 (KB 4054176)
<a href="#">KB4056897</a>	January 3, 2018—KB4056897 (Security-only update) Applies to: Windows Server 2008 R2 Service Pack 1, Windows 7 Service Pack 1
<a href="#">KB4073578</a>	Unbootable state for AMD devices in Windows 7 SP1 and Windows Server 2008 R2 SP1
<a href="#">KB4058043</a>	Microsoft Store reliability improvements for Windows 10 Version 1709: December 15, 2017
<a href="#">KB4056892</a>	January 3, 2018—KB4056892 (OS Build 16299.192) Applies to: Windows 10 version 1709
<a href="#">KB4056887</a>	Security update for Adobe Flash Player: January 9, 2018

## 2017 -Microsoft® Windows Patches Tested with MAXPRO®VMS/NVR

### December - 2017- Microsoft® Windows Patches Tested with MAXPRO®VMS/NVR

### November - 2017- Microsoft® Windows Patches Tested with MAXPRO®VMS/NVR

### October - 2017- Microsoft® Windows Patches Tested with MAXPRO®VMS/NVR

<b>Microsoft Knowledge Base Article ID</b>	<b>Description</b>
<a href="#">KB4057247</a>	Reliability update for upgrading to Windows 10 Version 1709: December 12, 2017
<a href="#">KB4055994</a>	Compatibility update for upgrading to and recovering Windows 10 Version 1709: December 12, 2017
<a href="#">KB4055237</a>	Compatibility update for upgrading to and recovering Windows 10 Version 1709: November 30, 2017
<a href="#">KB4054522</a>	December 12, 2017—KB4054522 (Security-only update) Applies to: Windows Server 2012 R2 Standard, Windows 8.1
<a href="#">KB4054521</a>	December 12, 2017—KB4054521 (Security-only update) Applies to: Windows 7 Service Pack 1, Windows Server 2008 R2 Service Pack 1
<a href="#">KB4054519</a>	December 12, 2017—KB4054519 (Monthly Rollup) Applies to: Windows 8.1, Windows Server 2012 R2 Standard
<a href="#">KB4054518</a>	December 12, 2017—KB4054518 (Monthly Rollup) Applies to: Windows Server 2008 R2 Service Pack 1, Windows 7 Service Pack 1
<a href="#">KB4054517</a>	December 12, 2017—KB4054517 (OS Build 16299.125) Applies to: Windows 10, Windows 10 version 1709
<a href="#">KB4053577</a>	Security update for Adobe Flash Player: December 12, 2017
<a href="#">KB4052978</a>	Cumulative security update for Internet Explorer: December 12, 2017

<b>Microsoft Knowledge Base Article ID</b>	<b>Description</b>
<a href="#">KB4047206</a>	Cumulative security update for Internet Explorer: November 14, 2017
<a href="#">KB4048960</a>	November 14, 2017—KB4048960 (Security-only update)
<a href="#">KB958488</a>	An update is available for Microsoft .NET Framework 3.5 Service Pack 1 on Windows 7 and Windows Server 2008 R2
<a href="#">KB4048957</a>	November 14, 2017—KB4048957 (Monthly Rollup)
<a href="#">KB4041777</a>	Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, and 4.7 for Windows 8.1, Windows RT 8.1 and Windows Server 2012 R2 (KB 4041777)
<a href="#">KB4043763</a>	Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, and 4.7 for Windows 8.1, Windows RT 8.1 and Windows Server 2012 R2 (KB 4043763)
<a href="#">KB4048951</a>	Security update for Adobe Flash Player: November 14, 2017
<a href="#">KB4048958</a>	November 14, 2017—KB4048958 (Monthly Rollup)
<a href="#">KB3161102</a>	Update for Windows Journal component removal
<a href="#">KB4033631</a>	Update to Windows 10 Version 1703, Version 1607, Version 1511, and Version 1507 for update applicability: November 16, 2017

Microsoft Knowledge Base Article ID	Description
<a href="#">KB4040685</a>	Cumulative security update for Internet Explorer: October 10, 2017
<a href="#">KB4041678</a>	This security update includes quality improvements. No new operating system features are being introduced in this update
<a href="#">KB2533552</a>	An update that prevents a "0xC0000034" error message when you try to install Windows 7 SP1, Windows Server 2008 R2 SP1, or Windows Embedded Standard 7 SP1 is available
<a href="#">KB976932</a>	Information about Service Pack 1 for Windows 7 and for Windows Server 2008 R2
<a href="#">KB4041681</a>	This security update includes improvements and fixes that were a part of update KB4038803 (released September 19, 2017)
<a href="#">KB4041687</a>	October 10, 2017—KB4041687 (Security-only update)
<a href="#">KB4041693</a>	This security update includes improvements and fixes that were a part of update KB4038774
<a href="#">KB3125217</a>	Disk cleanup for Windows 10 cumulative updates
<a href="#">KB3172729</a>	MS16-100: Description of the security update for Secure Boot
<a href="#">KB3173427</a>	Servicing stack update for Windows 10
<a href="#">KB4022730</a>	Security update for Adobe Flash Player
<a href="#">KB4022727</a>	This security update includes quality improvements. No new operating system features are being introduced in this update

# September - 2017- Microsoft® Windows Patches Tested with MAXPRO® VMS/NVR

Microsoft Knowledge Base Article ID	Description
<a href="#">KB4036586</a>	Cumulative security update for Internet Explorer: September 12, 2017
<a href="#">KB4038779</a>	This security update includes quality improvements. No new operating system features are being introduced in this update. September 12, 2017—KB4038779 (Security-only update)
<a href="#">KB4040980</a>	Description of the Security and Quality Rollup for the .NET Framework 3.5.1 for Windows 7 SP1 and Windows Server 2008 R2 SP1: September 12, 2017
<a href="#">KB4038777</a>	This security update includes improvements and fixes that were a part of update KB4034670 (released August 15, 2017)
<a href="#">KB4038793</a>	This security update includes quality improvements. No new operating system features are being introduced in this update September 12, 2017—KB4038793 (Security-only update)
<a href="#">KB4038806</a>	Security update for Adobe Flash Player: September 12, 2017
<a href="#">KB4040956</a>	Description of the Security Only update for the .NET Framework 4.6, 4.6.1, 4.6.2, and 4.7 for Windows 8.1, Windows RT 8.1 and Windows Server 2012 R2: September 12, 2017
<a href="#">KB4040967</a>	Description of the Security Only update for the .NET Framework 3.5 for Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2: September 12, 2017
<a href="#">KB4040972</a>	Description of the Security and Quality Rollup for the .NET Framework 4.6, 4.6.1, 4.6.2 and 4.7 for Windows 8.1, Windows RT 8.1 and Windows Server 2012 R2: September 12, 2017
<a href="#">KB4040981</a>	Description of the Security and Quality Rollup for the .NET Framework 3.5 for Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2: September 12, 2017
<a href="#">KB4038774</a>	This non-security update includes improvements and fixes that were a part of KB4038792 (released September 12, 2017). September 19, 2017—KB4038774 (Preview of Monthly Rollup)
<a href="#">KB4040724</a>	This update includes quality improvements. No new operating system features are being introduced in this update September 25, 2017—KB4040724 (OS Build 15063.632)

# August - 2017- Microsoft® Windows Patches Tested with MAXPRO® VMS/NVR

Microsoft KnowledgeBase Article ID	Description
<a href="#">KB4034674</a>	August 8, 2017—KB4034674 (OS Build 15063.540)
<a href="#">KB4034663</a>	August 15, 2017—KB4034663 (Preview of Monthly Rollup)
<a href="#">KB4034662</a>	Security update for Adobe Flash Player: August 8, 2017
<a href="#">KB4033997</a>	Description of Preview of Quality Rollup for the .NET Framework 3.5 for Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2: August 15, 2017
<a href="#">KB4033989</a>	Description of Preview of Quality Rollup for the .NET Framework 4.6, 4.6.1, 4.6.2, and 4.7 for Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2: August 15, 2017
<a href="#">KB4034664</a>	August 8, 2017—KB4034664 (Monthly Rollup)
<a href="#">KB4033996</a>	Description of Preview of Quality Rollup for the .NET Framework 3.5.1 for Windows 7 SP1 and Windows Server 2008 R2 SP1: August 15, 2017

# 2017 -Microsoft® Windows Patches Tested with MAXPRO®VMS/ NVR

Microsoft KnowledgeBase Article ID	Description
<a href="#">KB4025341</a>	July 11, 2017—KB4025341 (Monthly Rollup)
<a href="#">KB4033428</a>	Windows Server 2012 R2 processor generation detection reliability update: July 18, 2017
<a href="#">KB4025335</a>	July 18, 2017—KB4025335 (Preview of Monthly Rollup)
<a href="#">KB4025339</a>	July 11, 2017—KB4025339 (OS Build 14393.1480)
<a href="#">KB4025376</a>	Security update for Adobe Flash Player: July 11, 2017
<a href="#">KB4022719</a>	June 13, 2017—KB4022719 (Monthly Rollup). This security update includes improvements and fixes that were a part of update KB4019265 (released May 16, 2017)
<a href="#">KB3186539</a>	The Microsoft .NET Framework 4.7 for Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2
<a href="#">KB4022726</a>	June 13, 2017—KB4022726 (Monthly Rollup) This security update includes improvements and fixes that were a part of update ?KB4019217 (released May 16th, 2017)
<a href="#">KB4022715</a>	June 13, 2017—KB4022715 (OS Build 14393.1358) This security update includes quality improvements. No new operating system features are being introduced in this update.
<a href="#">KB4023834</a>	Servicing Stack Update for Windows 10 1607 and Windows Server 2016: June 13, 2017
<a href="#">KB4022730</a>	Security update for Adobe Flash Player: June 13, 2017
<a href="#">KB3186568</a>	The Microsoft .NET Framework 4.7 for Windows 10 Version 1607 and Windows Server 2016
<a href="#">KB4019990</a>	Update for the d3dcompiler_47.dll component on Windows Server 2012, Windows 7, and Windows Server 2008 R2
<a href="#">KB4014596</a>	May 2017 Description of the Quality Rollup for the .NET Framework 3.5.1 for Windows 7 SP1 and Windows Server 2008 R2 SP1 (KB4014596): May 16, 2017
<a href="#">KB4019472</a>	May 9, 2017—KB4019472 (OS Build 14393.1198)
<a href="#">KB3150513</a>	Latest compatibility definition update for Windows
<a href="#">KB4019264</a>	May 9, 2017—KB4019264 (Monthly Rollup)
<a href="#">KB4014504</a>	Description of the Security and Quality Rollup for the .NET Framework 3.5.1 for Windows 7 and Windows Server 2008 R2: May 9, 2017
<a href="#">KB4019217</a>	May 16, 2017—KB4019217 (Preview of Monthly Rollup)
<a href="#">KB4020821</a>	Security update for Adobe Flash Player: May 9, 2017
<a href="#">KB4014604</a>	May 2017 Description of the Quality Rollup for the .NET Framework 4.6, 4.6.1, and 4.6.2 for Windows 8.1 and Windows Server 2012 R2 (KB4014604): May 16, 2017
<a href="#">KB4014598</a>	May 2017 Description of the Quality Rollup for the .NET Framework 3.5 for Windows 8.1 and Windows Server 2012 R2 (KB4014598): May 16, 2017

<b>Microsoft KnowledgeBase Article ID</b>	<b>Description</b>
<a href="#">KB4014510</a>	Description of the Security and Quality Rollup for the .NET Framework 4.6 and 4.6.1 for Windows 8.1 and Windows Server 2012 R2: May 9, 2017
<a href="#">KB4014505</a>	Description of the Security and Quality Rollup for the .NET Framework 3.5 Service Pack 1 for Windows 8.1 and Windows Server 2012 R2: May 9, 2017
<a href="#">KB4012219</a>	March 2017 Preview of Monthly Quality Rollup for Windows 8.1 and Windows Server 2012 R2
<a href="#">KB4015438</a>	This update includes quality improvements. No new operating system features are being introduced in this update.
<a href="#">KB4013418</a>	This update makes stability improvements for the Windows 10 Version 1607 and Windows Server 2016 servicing stack.
<a href="#">KB4012215</a>	March 2017 Security Monthly Quality Rollup for Windows 7 SP1 and Windows Server 2008 R2 SP1
<a href="#">MS17-023</a>	Security Update for Adobe Flash Player (4014329)
<a href="#">MS17-022</a>	Security Update for Microsoft XML Core Services (4010321)
<a href="#">MS17-021</a>	Security Update for Windows DirectShow (4010318)
<a href="#">MS17-020</a>	Security Update for Windows DVD Maker (3208223)
<a href="#">MS17-019</a>	Security Update for Active Directory Federation Services (4010320)
<a href="#">MS17-018</a>	Security Update for Windows Kernel-Mode Drivers (4013083)
<a href="#">MS17-017</a>	Security Update for Windows Kernel (4013081)
<a href="#">MS17-016</a>	Security Update for Windows IIS (4013074)
<a href="#">MS17-015</a>	Security Update for Microsoft Exchange Server (4013242)
<a href="#">MS17-014</a>	Security Update for Microsoft Office (4013241)
<a href="#">MS17-013</a>	Security Update for Microsoft Graphics Component (4013075)
<a href="#">MS17-012</a>	Security Update for Microsoft Windows (4013078)
<a href="#">MS17-011</a>	Security Update for Microsoft Uniscribe (4013076)
<a href="#">MS17-010</a>	Security Update for Microsoft Windows SMB Server (4013389)
<a href="#">MS17-009</a>	Security Update for Microsoft Windows PDF Library (4010319)
<a href="#">MS17-008</a>	Security Update for Windows Hyper-V (4013082)
<a href="#">MS17-007</a>	Cumulative Security Update for Microsoft Edge (4013071)
<a href="#">MS17-006</a>	Cumulative Security Update for Internet Explorer (4013073)
<a href="#">MS17-005</a>	Security Update for Adobe Flash Player (4010250)
<a href="#">MS17-004</a>	Security Update for Local Security Authority Subsystem Service (3216771)
<a href="#">MS17-003</a>	Security Update for Adobe Flash Player (3214628)
<a href="#">MS17-002</a>	Security Update for Microsoft Office (3214291)
<a href="#">MS17-001</a>	Security Update for Microsoft Edge (3214288)

Microsoft KnowledgeBase Article ID	Description
<a href="#">KB3211320</a>	Servicing stack update for Windows 10 Version 1607 and Windows Server 2016: January 24, 2017
<a href="#">KB4009938</a>	January 10, 2017—KB3213986 (OS Build 14393.693)
<a href="#">KB3212646</a>	January 2017 Security Monthly Quality Rollup for Windows 7 SP1 and Windows Server 2008 R2 SP1

**2016 -Microsoft® Windows Patches Tested with MAXPRO®VMS/  
NVR**

**2016 - Microsoft® Windows Patches Tested with MAXPRO®NVR**

**2015 - Microsoft® Windows Patches Tested with MAXPRO®NVR**

**2014- Microsoft® Windows Patches Tested with  
MAXPRO®NVR**

**2013- Microsoft® Windows Patches Tested with  
MAXPRO®NVR**

**2016 -Windows 7, 32 Bit - Microsoft® Windows Patches Tested with  
MAXPRO®VMS**

**2016 -Windows 7, 64 Bit - Microsoft® Windows Patches Tested with  
MAXPRO®VMS**

**2016 -Windows 8.1, 64/32 Bit - Microsoft® Windows Patches  
Tested with MAXPRO®VMS**



<b>Microsoft KnowledgeBase Article ID</b>	<b>Description</b>
<a href="#">MS16-155</a>	Security Update for .NET Framework (3205640)
<a href="#">MS16-154</a>	Security Update for Adobe Flash Player (3209498)
<a href="#">MS16-153</a>	Security Update for Common Log File System Driver (3207328)
<a href="#">MS16-152</a>	Security Update for Windows Kernel (3199709)
<a href="#">MS16-151</a>	Security Update for Windows Kernel-Mode Drivers (3205651)
<a href="#">MS16-150</a>	Security Update for Secure Kernel Mode (3205642)
<a href="#">MS16-149</a>	Security Update for Microsoft Windows (3205655)
<a href="#">MS16-148</a>	Security Update for Microsoft Office (3204068)
<a href="#">MS16-147</a>	Security Update for Microsoft Uniscribe (3204063)
<a href="#">MS16-146</a>	Security Update for Microsoft Graphics Component (3204066)
<a href="#">MS16-145</a>	Cumulative Security Update for Microsoft Edge (3204062)
<a href="#">MS16-144</a>	Cumulative Security Update for Internet Explorer (3204059)
<a href="#">MS16-142</a>	Cumulative Security Update for Internet Explorer (3198467)
<a href="#">MS16-141</a>	Security Update for Adobe Flash Player (3202790)
<a href="#">MS16-140</a>	Security Update for Boot Manager (3193479)
<a href="#">MS16-139</a>	Security Update for Windows Kernel (3199720)
<a href="#">MS16-138</a>	Security Update to Microsoft Virtual Hard Disk Driver (3199647)
<a href="#">MS16-137</a>	Security Update for Windows Authentication Methods (3199173)
<a href="#">MS16-136</a>	Security Update for SQL Server (3199641)
<a href="#">MS16-135</a>	Security Update for Windows Kernel-Mode Drivers (3199135)
<a href="#">MS16-134</a>	Security Update for Common Log File System Driver (3193706)
<a href="#">MS16-133</a>	Security Update for Microsoft Office (3199168)
<a href="#">MS16-132</a>	Security Update for Microsoft Graphics Component (3199120)
<a href="#">MS16-131</a>	Security Update for Microsoft Video Control (3199151)
<a href="#">MS16-130</a>	Security Update for Microsoft Windows (3199172)
<a href="#">MS16-129</a>	Cumulative Security Update for Microsoft Edge (3199057)
<a href="#">MS16-128</a>	Security Update for Adobe Flash Player (3201860)
<a href="#">MS16-127</a>	Security Update for Adobe Flash Player (3194343)
<a href="#">MS16-126</a>	Security Update for Microsoft Internet Messaging API (3196067)
<a href="#">MS16-125</a>	Security Update for Diagnostics Hub (3193229)
<a href="#">MS16-124</a>	Security Update for Windows Registry (3193227)
<a href="#">MS16-123</a>	Security Update for Windows Kernel-Mode Drivers (3192892)
<a href="#">MS16-122</a>	Security Update for Microsoft Video Control (3195360)

<b>Microsoft KnowledgeBase Article ID</b>	<b>Description</b>
<a href="#">MS16-121</a>	Security Update for Microsoft Office (3194063)
<a href="#">MS16-120</a>	Security Update for Microsoft Graphics Component (3192884)
<a href="#">MS16-119</a>	Cumulative Security Update for Microsoft Edge (3192890)
<a href="#">MS16-118</a>	Cumulative Security Update for Internet Explorer (3192887)
<a href="#">MS16-117</a>	Security Update for Adobe Flash Player (3188128)
<a href="#">MS16-116</a>	Security Update in OLE Automation for VBScript Scripting Engine (3188724)
<a href="#">MS16-115</a>	Security Update for Microsoft Windows PDF Library (3188733)
<a href="#">MS16-114</a>	Security Update for SMBv1 Server (3185879)
<a href="#">MS16-113</a>	Security Update for Windows Secure Kernel Mode (3185876)
<a href="#">MS16-112</a>	Security Update for Windows Lock Screen (3178469)
<a href="#">MS16-111</a>	Security Update for Windows Kernel (3186973)
<a href="#">MS16-110</a>	Security Update for Windows (3178467)
<a href="#">MS16-109</a>	Security Update for Silverlight (3182373)
<a href="#">MS16-108</a>	Security Update for Microsoft Exchange Server (3185883)
<a href="#">MS16-107</a>	Security Update for Microsoft Office (3185852)
<a href="#">MS16-106</a>	Security Update for Microsoft Graphics Component (3185848)
<a href="#">MS16-105</a>	Cumulative Security Update for Microsoft Edge (3183043)
<a href="#">MS16-104</a>	Cumulative Security Update for Internet Explorer (3183038)

<b>Microsoft KnowledgeBase Article ID</b>	<b>Description</b>
<a href="#">MS16-103</a>	Security Update for ActiveSyncProvider (3182332)
<a href="#">MS16-102</a>	Security Update for Microsoft Windows PDF Library (3182248)
<a href="#">MS16-101</a>	Security Update for Windows Authentication Methods (3178465)
<a href="#">MS16-100</a>	Security Update for Secure Boot (3179577)
<a href="#">MS16-099</a>	Security Update for Microsoft Office (3177451)
<a href="#">MS16-098</a>	Security Update for Windows Kernel-Mode Drivers (3178466)
<a href="#">MS16-097</a>	Security Update for Microsoft Graphics Component (3177393)
<a href="#">MS16-096</a>	Cumulative Security Update for Microsoft Edge (3177358)
<a href="#">MS16-095</a>	Cumulative Security Update for Internet Explorer (3177356)
<a href="#">MS16-094</a>	Security Update for Secure Boot (3177404)
<a href="#">MS16-093</a>	Security Update for Adobe Flash Player (3174060)
<a href="#">MS16-092</a>	Security Update for Windows Kernel (3171910)

<b>Microsoft KnowledgeBase Article ID</b>	<b>Description</b>
<a href="#">MS16-091</a>	Security Update for .NET Framework (3170048)
<a href="#">MS16-090</a>	Security Update for Windows Kernel-Mode Drivers (3171481)
<a href="#">MS16-089</a>	Security Update for Windows Secure Kernel Mode (3170050)
<a href="#">MS16-088</a>	Security Update for Microsoft Office (3170008)
<a href="#">MS16-087</a>	Security Update for Windows Print Spooler Components (3170005)
<a href="#">MS16-086</a>	Cumulative Security Update for JScript and VBScript (3169996)
<a href="#">MS16-085</a>	Cumulative Security Update for Microsoft Edge (3169999)
<a href="#">MS16-084</a>	Cumulative Security Update for Internet Explorer (3169991)
<a href="#">MS16-083</a>	Security Update for Adobe Flash Player (3167685)
<a href="#">MS16-082</a>	Security Update for Microsoft Windows Search Component (3165270)
<a href="#">MS16-081</a>	Security Update for Active Directory (3160352)
<a href="#">MS16-080</a>	Security Update for Microsoft Windows PDF (3164302)
<a href="#">MS16-079</a>	Security Update for Microsoft Exchange Server (3160339)
<a href="#">MS16-078</a>	Security Update for Windows Diagnostic Hub (3165479)
<a href="#">MS16-077</a>	Security Update for WPAD (3165191)
<a href="#">MS16-076</a>	Security Update for Netlogon (3167691)
<a href="#">MS16-075</a>	Security Update for Windows SMB Server (3164038)
<a href="#">MS16-074</a>	Security Update for Microsoft Graphics Component (3164036)
<a href="#">MS16-073</a>	Security Update for Windows Kernel-Mode Drivers (3164028)
<a href="#">MS16-072</a>	Security Update for Group Policy (3163622)
<a href="#">MS16-071</a>	Security Update for Microsoft Windows DNS Server (3164065)
<a href="#">MS16-070</a>	Security Update for Microsoft Office (3163610)
<a href="#">MS16-069</a>	Cumulative Security Update for JScript and VBScript (3163640)
<a href="#">MS16-068</a>	Cumulative Security Update for Microsoft Edge (3163656)
<a href="#">MS16-067</a>	Security Update for Volume Manager Driver (3155784)
<a href="#">MS16-066</a>	Security Update for Virtual Secure Mode (3155451)
<a href="#">MS16-065</a>	Security Update for .NET Framework (3156757)
<a href="#">MS16-064</a>	Security Update for Adobe Flash Player (3157993)
<a href="#">MS16-063</a>	Cumulative Security Update for Internet Explorer (3163649)
<a href="#">MS16-062</a>	Security Update for Windows Kernel-Mode Drivers (3158222)
<a href="#">MS16-061</a>	Security Update for Microsoft RPC (3155520)
<a href="#">MS16-060</a>	Security Update for Windows Kernel (3154846)
<a href="#">MS16-059</a>	Security Update for Windows Media Center (3150220)

<b>Microsoft KnowledgeBase Article ID</b>	<b>Description</b>
<a href="#">MS16-058</a>	Security Update for Windows IIS (3141083)
<a href="#">MS16-057</a>	Security Update for Windows Shell (3156987)
<a href="#">MS16-056</a>	Security Update for Windows Journal (3156761)
<a href="#">MS16-055</a>	Security Update for Microsoft Graphics Component (3156754)
<a href="#">MS16-054</a>	Security Update for Microsoft Office (3155544)
<a href="#">MS16-053</a>	Cumulative Security Update for JScript and VBScript (3156764)
<a href="#">MS16-052</a>	Cumulative Security Update for Microsoft Edge (3155538)
<a href="#">MS16-051</a>	Cumulative Security Update for Internet Explorer (3155533)
<a href="#">MS16-050</a>	Security Update for Adobe Flash Player (3154132)
<a href="#">MS16-049</a>	Security Update for HTTP.sys (3148795)
<a href="#">MS16-048</a>	Security Update for CSRSS (3148528)
<a href="#">MS16-047</a>	Security Update for SAM and LSAD Remote Protocols (3148527)
<a href="#">MS16-046</a>	Security Update for Secondary Logon (3148538)
<a href="#">MS16-045</a>	Security Update for Windows Hyper-V (3143118)
<a href="#">MS16-044</a>	Security Update for Windows OLE (3146706)
<a href="#">MS16-042</a>	Security Update for Microsoft Office (3148775)
<a href="#">MS16-041</a>	Security Update for .NET Framework (3148789)
<a href="#">MS16-040</a>	Security Update for Microsoft XML Core Services (3148541)
<a href="#">MS16-039</a>	Security Update for Microsoft Graphics Component (3148522)
<a href="#">MS16-038</a>	Cumulative Security Update for Microsoft Edge (3148532)
<a href="#">MS16-037</a>	Cumulative Security Update for Internet Explorer (3148531)
<a href="#">MS16-036</a>	Security Update for Adobe Flash Player (3144756)
<a href="#">MS16-035</a>	Security Update for .NET Framework to Address Security Feature Bypass (3141780)
<a href="#">MS16-034</a>	Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege (3143145)
<a href="#">MS16-033</a>	Security Update for Windows USB Mass Storage Class Driver to Address Elevation of Privilege (3143142)
<a href="#">MS16-032</a>	Security Update for Secondary Logon to Address Elevation of Privilege (3143141)
<a href="#">MS16-031</a>	Security Update for Microsoft Windows to Address Elevation of Privilege (3140410)
<a href="#">MS16-030</a>	Security Update for Windows OLE to Address Remote Code Execution (3143136)
<a href="#">MS16-029</a>	Security Update for Microsoft Office to Address Remote Code Execution (3141806)
<a href="#">MS16-028</a>	Security Update for Microsoft Windows PDF Library to Address Remote Code Execution (3143081)
<a href="#">MS16-027</a>	Security Update for Windows Media to Address Remote Code Execution (3143146)

<b>Microsoft KnowledgeBase Article ID</b>	<b>Description</b>
<a href="#">MS16-026</a>	Security Update for Graphic Fonts to Address Remote Code Execution (3143148)
<a href="#">MS16-025</a>	Security Update for Windows Library Loading to Address Remote Code Execution (3140709)
<a href="#">MS16-024</a>	Cumulative Security Update for Microsoft Edge (3142019)
<a href="#">MS16-023</a>	Cumulative Security Update for Internet Explorer (3142015)
<a href="#">MS16-022</a>	Security Update for Adobe Flash Player (3135782)
<a href="#">MS16-021</a>	Security Update for NPS RADIUS Server to Address Denial of Service (3133043)
<a href="#">MS16-020</a>	Security Update for Active Directory Federation Services to Address Denial of Service (3134222)
<a href="#">MS16-019</a>	Security Update for .NET Framework to Address Denial of Service (3137893)
<a href="#">MS16-018</a>	Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege (3136082)
<a href="#">MS16-017</a>	Security Update for Remote Desktop Display Driver to Address Elevation of Privilege (3134700)
<a href="#">MS16-016</a>	Security Update for WebDAV to Address Elevation of Privilege (3136041)
<a href="#">MS16-015</a>	Security Update for Microsoft Office to Address Remote Code Execution (3134226)
<a href="#">MS16-014</a>	Security Update for Microsoft Windows to Address Remote Code Execution (3134228)
<a href="#">MS16-013</a>	Security Update for Windows Journal to Address Remote Code Execution (3134811)
<a href="#">MS16-012</a>	Security Update for Microsoft Windows PDF Library to Address Remote Code Execution (3138938)
<a href="#">MS16-011</a>	Cumulative Security Update for Microsoft Edge (3134225)
<a href="#">MS16-010</a>	Security Update in Microsoft Exchange Server to Address Spoofing (3124557)
<a href="#">MS16-009</a>	Cumulative Security Update for Internet Explorer (3134220)
<a href="#">MS16-008</a>	Security Update for Windows Kernel to Address Elevation of Privilege (3124605)
<a href="#">MS16-007</a>	Security Update for Microsoft Windows to Address Remote Code Execution (3124901)
<a href="#">MS16-006</a>	Security Update for Silverlight to Address Remote Code Execution (3126036)
<a href="#">MS16-005</a>	Security Update for Windows Kernel-Mode Drivers to Address Remote Code Execution (3124584)
<a href="#">MS16-004</a>	Security Update for Microsoft Office to Address Remote Code Execution (3124585)
<a href="#">MS16-003</a>	Cumulative Security Update for JScript and VBScript to Address Remote Code Execution (3125540)
<a href="#">MS16-002</a>	Cumulative Security Update for Microsoft Edge (3124904)
<a href="#">MS16-001</a>	Cumulative Security Update for Internet Explorer (3124903)

<b>Microsoft KnowledgeBase Article ID</b>	<b>Description</b>
<a href="#">MS15-135</a>	Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege (3119075)
<a href="#">MS15-134</a>	Security Update for Windows Media Center to Address Remote Code Execution (3108669)
<a href="#">MS15-133</a>	Security Update for Windows PGM to Address Elevation of Privilege (3116130)
<a href="#">MS15-132</a>	Security Update for Microsoft Windows to Address Remote Code Execution (3116162)
<a href="#">MS15-131</a>	Security Update for Microsoft Office to Address Remote Code Execution (3116111)
<a href="#">MS15-130</a>	Security Update for Microsoft Uniscribe to Address Remote Code Execution (3108670)
<a href="#">MS15-129</a>	Security Update for Silverlight to Address Remote Code Execution (3106614)
<a href="#">MS15-128</a>	Security Update for Microsoft Graphics Component to Address Remote Code Execution (3104503)
<a href="#">MS15-127</a>	Security Update for Microsoft Windows DNS to Address Remote Code Execution (3100465)
<a href="#">MS15-126</a>	Cumulative Security Update for JScript and VBScript to Address Remote Code Execution (3116178)
<a href="#">MS15-125</a>	Cumulative Security Update for Microsoft Edge (3116184)
<a href="#">MS15-124</a>	Cumulative Security Update for Internet Explorer (3116180)
<a href="#">MS15-123</a>	Security Update for Skype for Business and Microsoft Lync to Address Information Disclosure (3105872)
<a href="#">MS15-122</a>	Security Update for Kerberos to Address Security Feature Bypass (3105256)
<a href="#">MS15-121</a>	Security Update for Schannel to Address Spoofing (3081320)
<a href="#">MS15-120</a>	Security Update for IPsec to Address Denial of Service (3102939)
<a href="#">MS15-119</a>	Security Update for Winsock to Address Elevation of Privilege (3104521)
<a href="#">MS15-118</a>	Security Update for .NET Framework to Address Elevation of Privilege (3104507)
<a href="#">MS15-117</a>	Security Update for NDIS to Address Elevation of Privilege (3101722)
<a href="#">MS15-116</a>	Security Update for Microsoft Office to Address Remote Code Execution (3104540)
<a href="#">MS15-115</a>	Security Update for Microsoft Windows to Address Remote Code Execution (3105864)
<a href="#">MS15-114</a>	Security Update for Windows Journal to Address Remote Code Execution (3100213)
<a href="#">MS15-113</a>	Cumulative Security Update for Microsoft Edge (3104519)
<a href="#">MS15-112</a>	Cumulative Security Update for Internet Explorer (3104517)
<a href="#">MS15-111</a>	Security Update for Windows Kernel to Address Elevation of Privilege (3096447)
<a href="#">MS15-110</a>	Security Updates for Microsoft Office to Address Remote Code Execution (3096440)
<a href="#">MS15-109</a>	Security Update for Windows Shell to Address Remote Code Execution (3096443)
<a href="#">MS15-108</a>	Security Update for JScript and VBScript to Address Remote Code Execution (3089659)
<a href="#">MS15-107</a>	Cumulative Security Update for Microsoft Edge (3096448)

<a href="#">MS15-106</a>	<b>Cumulative Security Update for Internet Explorer (3096441)</b>
<a href="#">MS15-105</a>	<b>Vulnerability in Windows Hyper-V Could Allow Security Feature Bypass (3091287)</b>
<a href="#">MS15-104</a>	<b>Vulnerabilities in Skype for Business Server and Lync Server Could Allow Elevation of Privilege (3089952)</b>
<a href="#">MS15-103</a>	<b>Vulnerabilities in Microsoft Exchange Server Could Allow Information Disclosure (3089250)</b>
<a href="#">MS15-102</a>	<b>Vulnerabilities in Windows Task Management Could Allow Elevation of Privilege (3089657)</b>
<a href="#">MS15-101</a>	<b>Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (3089662)</b>
<a href="#">MS15-100</a>	<b>Vulnerability in Windows Media Center Could Allow Remote Code Execution (3087918)</b>
<a href="#">MS15-099</a>	<b>Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3089664)</b>
<a href="#">MS15-098</a>	<b>Vulnerabilities in Windows Journal Could Allow Remote Code Execution (3089669)</b>
<a href="#">MS15-097</a>	<b>Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (3089656)</b>
<a href="#">MS15-096</a>	<b>Vulnerability in Active Directory Service Could Allow Denial of Service (3072595)</b>
<a href="#">MS15-095</a>	<b>Cumulative Security Update for Microsoft Edge (3089665)</b>
<a href="#">MS15-094</a>	<b>Cumulative Security Update for Internet Explorer (3089548)</b>
<a href="#">MS15-093</a>	<b>Security Update for Internet Explorer (3088903)</b>
<a href="#">MS15-092</a>	<b>Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (3086251)</b>
<a href="#">MS15-091</a>	<b>Cumulative Security Update for Microsoft Edge (3084525)</b>
<a href="#">MS15-090</a>	<b>Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege (3060716)</b>
<a href="#">MS15-089</a>	<b>Vulnerability in WebDAV Could Allow Information Disclosure (3076949)</b>
<a href="#">MS15-088</a>	<b>Unsafe Command Line Parameter Passing Could Allow Information Disclosure (3082458)</b>
<a href="#">MS15-087</a>	<b>Vulnerability in UDDI Services Could Allow Elevation of Privilege (3082459)</b>
<a href="#">MS15-086</a>	<b>Vulnerability in System Center Operations Manager Could Allow Elevation of Privilege (3075158)</b>
<a href="#">MS15-085</a>	<b>Vulnerability in Mount Manager Could Allow Elevation of Privilege (3082487)</b>
<a href="#">MS15-084</a>	<b>Vulnerabilities in XML Core Services Could Allow Information Disclosure (3080129)</b>
<a href="#">MS15-083</a>	<b>Vulnerability in Server Message Block Could Allow Remote Code Execution (3073921)</b>
<a href="#">MS15-082</a>	<b>Vulnerabilities in RDP Could Allow Remote Code Execution (3080348)</b>
<a href="#">MS15-081</a>	<b>Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3080790)</b>
<a href="#">MS15-080</a>	<b>Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (3078662)</b>
<a href="#">MS15-079</a>	<b>Cumulative Security Update for Internet Explorer (3082442)</b>
<a href="#">MS15-078</a>	<b>Vulnerability in Microsoft Font Driver Could Allow Remote Code Execution (3079904)</b>
<a href="#">MS15-077</a>	<b>Vulnerability in ATM Font Driver Could Allow Elevation of Privilege (3077657)</b>
<a href="#">MS15-076</a>	<b>Vulnerability in Windows Remote Procedure Call Could Allow Elevation of Privilege (3067505)</b>

<a href="#">MS15-075</a>	<b>Vulnerabilities in OLE Could Allow Elevation of Privilege (3072633)</b>
<a href="#">MS15-074</a>	<b>Vulnerability in Windows Installer Service Could Allow Elevation of Privilege (3072630)</b>
<a href="#">MS15-073</a>	<b>Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (3070102)</b>
<a href="#">MS15-072</a>	<b>Vulnerability in Windows Graphics Component Could Allow Elevation of Privilege (3069392)</b>
<a href="#">MS15-071</a>	<b>Vulnerability in Netlogon Could Allow Elevation of Privilege (3068457)</b>
<a href="#">MS15-070</a>	<b>Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3072620)</b>
<a href="#">MS15-069</a>	<b>Vulnerabilities in Windows Could Allow Remote Code Execution (3072631)</b>
<a href="#">MS15-068</a>	<b>Vulnerabilities in Windows Hyper-V Could Allow Remote Code Execution (3072000)</b>
<a href="#">MS15-067</a>	<b>Vulnerability in RDP Could Allow Remote Code Execution (3073094)</b>
<a href="#">MS15-066</a>	<b>Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (3072604)</b>
<a href="#">MS15-065</a>	<b>Security Update for Internet Explorer (3076321)</b>
<a href="#">MS15-064</a>	<b>Vulnerabilities in Microsoft Exchange Server Could Allow Elevation of Privilege (3062157)</b>
<a href="#">MS15-063</a>	<b>Vulnerability in Windows Kernel Could Allow Elevation of Privilege (3063858)</b>
<a href="#">MS15-062</a>	<b>Vulnerability in Active Directory Federation Services Could Allow Elevation of Privilege (3062577)</b>
<a href="#">MS15-061</a>	<b>Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (3057839)</b>
<a href="#">MS15-060</a>	<b>Vulnerability in Microsoft Common Controls Could Allow Remote Code Execution (3059317)</b>
<a href="#">MS15-059</a>	<b>Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3064949)</b>
<a href="#">MS15-058</a>	<b>Vulnerabilities in SQL Server Could Allow Remote Code Execution (3065718)</b>
<a href="#">MS15-057</a>	<b>Vulnerability in Windows Media Player Could Allow Remote Code Execution (3033890)</b>
<a href="#">MS15-056</a>	<b>Cumulative Security Update for Internet Explorer (3058515)</b>
<a href="#">MS15-055</a>	<b>Vulnerability in Schannel Could Allow Information Disclosure (3061518)</b>
<a href="#">MS15-054</a>	<b>Vulnerability in Microsoft Management Console File Format Could Allow Denial of Service (3051768)</b>
<a href="#">MS15-053</a>	<b>Vulnerabilities in JScript and VBScript Scripting Engines Could Allow Security Feature Bypass (3057263)</b>
<a href="#">MS15-052</a>	<b>Vulnerability in Windows Kernel Could Allow Security Feature Bypass (3050514)</b>
<a href="#">MS15-051</a>	<b>Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (3057191)</b>
<a href="#">MS15-050</a>	<b>Vulnerability in Service Control Manager Could Allow Elevation of Privilege (3055642)</b>
<a href="#">MS15-049</a>	<b>Vulnerability in Silverlight Could Allow Elevation of Privilege (3058985)</b>
<a href="#">MS15-048</a>	<b>Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (3057134)</b>
<a href="#">MS15-047</a>	<b>Vulnerabilities in Microsoft SharePoint Server Could Allow Remote Code Execution (3058083)</b>



<a href="#">MS15-046</a>	<b>Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3057181)</b>
<a href="#">MS15-045</a>	<b>Vulnerability in Windows Journal Could Allow Remote Code Execution (3046002)</b>
<a href="#">MS15-044</a>	<b>Vulnerabilities in Microsoft Font Drivers Could Allow Remote Code Execution (3057110)</b>
<a href="#">MS15-043</a>	<b>Cumulative Security Update for Internet Explorer (3049563)</b>
<a href="#">MS15-042</a>	<b>Vulnerability in Windows Hyper-V Could Allow Denial of Service (3047234)</b>
<a href="#">MS15-041</a>	<b>Vulnerability in .NET Framework Could Allow Information Disclosure (3048010)</b>
<a href="#">MS15-040</a>	<b>Vulnerability in Active Directory Federation Services Could Allow Information Disclosure (3045711)</b>
<a href="#">MS15-039</a>	<b>Vulnerability in XML Core Services Could Allow Security Feature Bypass (3046482)</b>
<a href="#">MS15-038</a>	<b>Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege (3049576)</b>
<a href="#">MS15-037</a>	<b>Vulnerability in Windows Task Scheduler Could Allow Elevation of Privilege (3046269)</b>
<a href="#">MS15-036</a>	<b>Vulnerabilities in Microsoft SharePoint Server Could Allow Elevation of Privilege (3052044)</b>
<a href="#">MS15-035</a>	<b>Vulnerability in Microsoft Graphics Component Could Allow Remote Code Execution (3046306)</b>
<a href="#">MS15-034</a>	<b>Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)</b>
<a href="#">MS15-033</a>	<b>Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3048019)</b>
<a href="#">MS15-032</a>	<b>Cumulative Security Update for Internet Explorer (3038314)</b>
<a href="#">MS15-031</a>	<b>Vulnerability in Schannel Could Allow Security Feature Bypass (3046049)</b>
<a href="#">MS15-030</a>	<b>Vulnerability in Remote Desktop Protocol Could Allow Denial of Service (3039976)</b>
<a href="#">MS15-029</a>	<b>Vulnerability in Windows Photo Decoder Component Could Allow Information Disclosure (3035126)</b>
<a href="#">MS15-028</a>	<b>Vulnerability in Windows Task Scheduler Could Allow Security Feature Bypass (3030377)</b>
<a href="#">MS15-027</a>	<b>Vulnerability in NETLOGON Could Allow Spoofing (3002657)</b>
<a href="#">MS15-026</a>	<b>Vulnerabilities in Microsoft Exchange Server Could Allow Elevation of Privilege (3040856)</b>
<a href="#">MS15-025</a>	<b>Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (3038680)</b>
<a href="#">MS15-024</a>	<b>Vulnerability in PNG Processing Could Allow Information Disclosure (3035132)</b>
<a href="#">MS15-023</a>	<b>Vulnerabilities in Kernel-Mode Driver Could Allow Elevation of Privilege (3034344)</b>
<a href="#">MS15-022</a>	<b>Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3038999)</b>
<a href="#">MS15-021</a>	<b>Vulnerabilities in Adobe Font Driver Could Allow Remote Code Execution (3032323)</b>
<a href="#">MS15-020</a>	<b>Vulnerabilities in Microsoft Windows Could Allow Remote Code Execution (3041836)</b>
<a href="#">MS15-019</a>	<b>Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (3040297)</b>
<a href="#">MS15-018</a>	<b>Cumulative Security Update for Internet Explorer (3032359)</b>
<a href="#">MS15-017</a>	<b>Vulnerability in Virtual Machine Manager Could Allow Elevation of Privilege (3035898)</b>

<a href="#">MS15-016</a>	Vulnerability in Microsoft Graphics Component Could Allow Information Disclosure (3029944)
<a href="#">MS15-015</a>	Vulnerability in Microsoft Windows Could Allow Elevation of Privilege (3031432)
<a href="#">MS15-014</a>	Vulnerability in Group Policy Could Allow Security Feature Bypass (3004361)
<a href="#">MS15-013</a>	Vulnerability in Microsoft Office Could Allow Security Feature Bypass (3033857)
<a href="#">MS15-012</a>	Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3032328)
<a href="#">MS15-011</a>	Vulnerability in Group Policy Could Allow Remote Code Execution (3000483)
<a href="#">MS15-010</a>	Vulnerabilities in Windows Kernel-Mode Driver Could Allow Remote Code Execution (3036220)
<a href="#">MS15-009</a>	Security Update for Internet Explorer (3034682)
<a href="#">MS15-008</a>	Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (3019215)
<a href="#">MS15-007</a>	Vulnerability in Network Policy Server RADIUS Implementation Could Cause Denial of Service (3014029)
<a href="#">MS15-006</a>	Vulnerability in Windows Error Reporting Could Allow Security Feature Bypass (3004365)
<a href="#">MS15-005</a>	Vulnerability in Network Location Awareness Service Could Allow Security Feature Bypass (3022777)
<a href="#">MS15-004</a>	Vulnerability in Windows Components Could Allow Elevation of Privilege (3025421)
<a href="#">MS15-003</a>	Vulnerability in Windows User Profile Service Could Allow Elevation of Privilege (3021674)
<a href="#">MS15-002</a>	Vulnerability in Windows Telnet Service Could Allow Remote Code Execution (3020393)
<a href="#">MS15-001</a>	Vulnerability in Windows Application Compatibility Cache Could Allow Elevation of Privilege (3023266)

<b>Microsoft KnowledgeBase Article ID</b>	<b>Description</b>
<a href="#">MS14-085</a>	Vulnerability in Microsoft Graphics Component Could Allow Information Disclosure (3013126)
<a href="#">MS14-084</a>	Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (3016711)
<a href="#">MS14-083</a>	Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (3017347)
<a href="#">MS14-082</a>	Vulnerability in Microsoft Office Could Allow Remote Code Execution (3017349)
<a href="#">MS14-081</a>	Vulnerabilities in Microsoft Word and Microsoft Office Web Apps Could Allow Remote Code Execution (3017301)
<a href="#">MS14-080</a>	Cumulative Security Update for Internet Explorer (3008923)
<a href="#">MS14-079</a>	Vulnerability in Kernel Mode Driver Could Allow Denial of Service (3002885)
<a href="#">MS14-078</a>	Vulnerability in IME (Japanese) Could Allow Elevation of Privilege (2992719)

<b>Microsoft KnowledgeBase Article ID</b>	<b>Description</b>
<a href="#">MS14-077</a>	Vulnerability in Active Directory Federation Services Could Allow Information Disclosure (3003381)
<a href="#">MS14-076</a>	Vulnerability in Internet Information Services (IIS) Could Allow Security Feature Bypass (2982998)
<a href="#">MS14-075</a>	Vulnerabilities in Microsoft Exchange Server Could Allow Elevation of Privilege (3009712)
<a href="#">MS14-074</a>	Vulnerability in Remote Desktop Protocol Could Allow Security Feature Bypass (3003743)
<a href="#">MS14-073</a>	Vulnerability in Microsoft SharePoint Foundation Could Allow Elevation of Privilege (3000431)
<a href="#">MS14-072</a>	Vulnerability in .NET Framework Could Allow Elevation of Privilege (3005210)
<a href="#">MS14-071</a>	Vulnerability in Windows Audio Service Could Allow Elevation of Privilege (3005607)
<a href="#">MS14-070</a>	Vulnerability in TCP/IP Could Allow Elevation of Privilege (2989935)
<a href="#">MS14-069</a>	Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3009710)
<a href="#">MS14-068</a>	Vulnerability in Kerberos Could Allow Elevation of Privilege (3011780)
<a href="#">MS14-067</a>	Vulnerability in XML Core Services Could Allow Remote Code Execution (2993958)
<a href="#">MS14-066</a>	Vulnerability in Schannel Could Allow Remote Code Execution (2992611)
<a href="#">MS14-065</a>	Cumulative Security Update for Internet Explorer (3003057)
<a href="#">MS14-064</a>	Vulnerabilities in Windows OLE Could Allow Remote Code Execution (3011443)
<a href="#">MS14-063</a>	Vulnerability in FAT32 Disk Partition Driver Could Allow Elevation of Privilege (2998579)
<a href="#">MS14-062</a>	Vulnerability in Message Queuing Service Could Allow Elevation of Privilege (2993254)
<a href="#">MS14-061</a>	Vulnerability in Microsoft Word and Office Web Apps Could Allow Remote Code Execution (3000434)
<a href="#">MS14-060</a>	Vulnerability in Windows OLE Could Allow Remote Code Execution (3000869)
<a href="#">MS14-059</a>	Vulnerability in ASP.NET MVC Could Allow Security Feature Bypass (2990942)
<a href="#">MS14-058</a>	Vulnerability in Kernel-Mode Driver Could Allow Remote Code Execution (3000061)
<a href="#">MS14-057</a>	Vulnerabilities in .NET Framework Could Allow Remote Code Execution (3000414)
<a href="#">MS14-056</a>	Cumulative Security Update for Internet Explorer (2987107)
<a href="#">MS14-055</a>	Vulnerabilities in Microsoft Lync Server Could Allow Denial of Service (2990928)
<a href="#">MS14-054</a>	Vulnerability in Windows Task Scheduler Could Allow Elevation of Privilege (2988948)
<a href="#">MS14-053</a>	Vulnerability in .NET Framework Could Allow Denial of Service (2990931)
<a href="#">MS14-052</a>	Cumulative Security Update for Internet Explorer (2977629)
<a href="#">KB2862152</a>	Microsoft security advisory: Vulnerability in IPsec could allow security feature bypass
<a href="#">KB2871997</a>	Microsoft Security Advisory: Update to improve credentials protection and management: May 13, 2014

<b>Microsoft KnowledgeBase Article ID</b>	<b>Description</b>
<a href="#">KB2898857</a>	MS14-009: Description of the security update for the .NET Framework 3.5.1 for Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1: February 11, 2014
<a href="#">KB2909210</a>	MS14-011: Description of the security update for Visual Basic Scripting Edition (VBScript) 5.8: February 11, 2014
<a href="#">KB2911501</a>	MS14-009: Description of the security update for the .NET Framework 3.5.1 for Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1: February 11, 2014
<a href="#">KB2922229</a>	Vulnerability in Windows file handling component could allow remote code execution: April 8, 2014
<a href="#">KB2926765</a>	MS14-027: Description of the security update for Windows: May 13, 2014
<a href="#">KB2929733</a>	The first stage of the WER protocol is not SSL encrypted in Windows
<a href="#">KB2931356</a>	MS14-026: Description of the security update for the .NET Framework 3.5.1 on Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1: May 13, 2014
<a href="#">KB2939576</a>	MS14-033: Description of the security update for MSXML: June 10, 2014
<a href="#">KB2957189</a>	MS14-031: Description of the security update for TCP for Windows: June 10, 2014
<a href="#">KB2957503</a>	MS14-036: Description of the security update for Windows 7, Windows Server 2008 R2, Windows Server 2008, Windows Vista, and Windows Server 2003: June 10, 2014
<a href="#">KB2957509</a>	MS14-036: Description of the security update for Windows 7, Windows Server 2008 R2, Windows Server 2008, Windows Vista, and Windows Server 2003: June 10, 2014
<a href="#">KB2961072</a>	MS14-040: Description of the security update for an ancillary function driver: July 8, 2014
<a href="#">KB2962872</a>	MS14-037: Security update for Internet Explorer versions 6, 7, 8, 9, 10, and 11: July 8, 2014
<a href="#">KB2971850</a>	MS14-038: Description of the security update for Windows: July 8, 2014
<a href="#">KB2972280</a>	MS14-041: Description of the security update for DirectShow: July 8, 2014
<a href="#">KB2973201</a>	MS14-039: Description of the security update for Windows on-screen keyboard: July 8, 2014
<a href="#">KB2973351</a>	Microsoft Security Advisory: Registry update to improve credentials protection and management for Windows-based systems that have the 2919355 update installed: July 8, 2014

<b>Microsoft KnowledgeBase Article ID</b>	<b>Description</b>
<a href="#">KB2798162</a>	Update to improve messaging in dialog boxes when you run executable files in Windows.
<a href="#">KB2813430</a>	Enables administrators to update trusted and disallowed CTLs in disconnected environments in Windows
<a href="#">KB2832414</a>	MS13-052: Description of the security update for the .NET Framework 3.5.1 on Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1: July 9, 2013
<a href="#">KB2836942</a>	Update for the .NET Framework 3.5.1 on Windows 7 SP1 and Windows Server 2008 R2 SP1 (June 2013)
<a href="#">KB2836943</a>	Update for the .NET Framework 3.5.1 on Windows 7 SP1 and Windows Server 2008 R2 SP1: September 2013

Microsoft KnowledgeBase Article ID	Description
<a href="#">KB2839894</a>	MS13-050: Vulnerability in Windows print spooler components could allow elevation of privilege: June 11, 2013
<a href="#">KB2840631</a>	MS13-052: Description of the security update for the .NET Framework 3.5.1 on Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1: July 9, 2013
<a href="#">KB2847311</a>	MS13-081: Description of the security update for kernel-mode drivers: October 8, 2013
<a href="#">KB2847927</a>	MS13-058: Vulnerability in Windows Defender could allow elevation of privilege: July 9, 2013
<a href="#">KB2855844</a>	MS13-081: Description of the security update for kernel-mode drivers: October 8, 2013
<a href="#">KB2861191</a>	MS13-082: Description of the security update for the .NET Framework 3.5.1 on Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1: October 8, 2013
<a href="#">KB2861855</a>	Microsoft Security Advisory: Updates to improve Remote Desktop Protocol network-level authentication: August 13, 2013
<a href="#">KB2862330</a>	MS13-081: Description of the security update for USB drivers: October 8, 2013
<a href="#">KB2862335</a>	MS13-081: Description of the security update for USB drivers: October 8, 2013
<a href="#">KB2862966</a>	An update is available that improves management of weak certificate cryptographic algorithms in Windows
<a href="#">KB2862973</a>	Microsoft Security Advisory: Update for deprecation of MD5 hashing algorithm for Microsoft root certificate program: August 13, 2013
<a href="#">KB2864058</a>	MS13-083: Vulnerability in Windows Common Control Library could allow remote code execution: October 8, 2013
<a href="#">KB2864202</a>	MS13-081: Description of the security update for USB drivers: October 8, 2013
<a href="#">KB2868038</a>	MS13-081: Description of the security update for USB drivers: October 8, 2013
<a href="#">KB2868626</a>	MS13-095: Vulnerability in XML digital signatures could allow denial of service: November 12, 2013
<a href="#">KB2876284</a>	MS13-081: Description of the security update for kernel-mode drivers: October 8, 2013
<a href="#">KB2876331</a>	MS13-089: Vulnerability in Windows Graphics Device Interface could allow remote code execution: November 12, 2013
<a href="#">KB2884256</a>	MS13-081: Description of the security update for USB drivers: October 8, 2013
<a href="#">KB2887069</a>	MS13-101: Description of the security update for Windows kernel-mode drivers: December 10, 2013
<a href="#">KB2892074</a>	MS13-099: Description of the security update for Windows Script 5.8: December 10, 2013
<a href="#">KB2893294</a>	MS13-098: Vulnerability in Windows could allow remote code execution: December 10, 2013
<a href="#">KB2900986</a>	MS13-090: Cumulative security update for ActiveX Kill Bits: November 12, 2013
<a href="#">KB958488</a>	An update is available for Microsoft .NET Framework 3.5 Service Pack 1 on Windows 7 and Windows Server 2008 R2
<a href="#">KB976902</a>	An update that prevents a "0xC0000034" error message when you try to install Windows 7 SP1, Windows Server 2008 R2 SP1, or Windows Embedded Standard 7 SP1 is available

Microsoft KnowledgeBase Article ID	Description
<a href="#">Kb2534111</a>	Computer name cannot contain only numbers" error message when you install Windows 7 by using Windows 7 SP1 integrated installation media
<a href="#">MS15-088</a>	This security update helps resolve an information disclosure vulnerability in Windows, Internet Explorer, and Microsoft Office. To exploit the vulnerability, an attacker would first have to use another vulnerability in Internet Explorer to run code in the sandboxed process. The attacker could then run Notepad, Visio, PowerPoint, Excel, or Word by using an unsafe command-line parameter to effect information disclosure. To be protected from the vulnerability, customers must apply the updates that are provided in this bulletin and also the update for Internet Explorer that is provided in MS15-079. Similarly, customers who are running an affected Office product must also install the applicable updates that are provided in MS15-081.
<a href="#">MS15-090</a>	Vulnerabilities in Windows could allow elevation of privilege.
<a href="#">MS15-085</a>	This security update resolves a vulnerability in Windows that could allow elevation of privilege if an attacker inserts a malicious USB device into a target system. An attacker could then write a malicious binary to disk and execute the code.
<a href="#">MS15-080</a>	This security update resolves vulnerabilities in the Microsoft .NET Framework and Microsoft Silverlight. These vulnerabilities could allow remote code execution if a user opens a specially crafted document or goes to an untrusted webpage that contains embedded TrueType or OpenType fonts.
<a href="#">MS15-101</a>	This update resolves vulnerabilities in the Microsoft .NET Framework that could allow elevation of privilege if a user runs a specially crafted .NET Framework application.
<a href="#">MS15-082</a>	This security update resolves vulnerabilities in Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker first places a specially crafted dynamic link library (DLL) file in the target user's current working directory and then convinces the user to open an RDP file or to launch a program that is designed to load a trusted DLL file but instead loads the attacker's specially crafted DLL file. An attacker who successfully exploited the vulnerabilities could take complete control of an affected system. An attacker could then install programs, could view, change, or delete data, or could create new accounts that have full user rights.
<a href="#">MS15-084</a>	This security update resolves vulnerabilities in Microsoft Windows and Microsoft Office. The vulnerabilities could allow information disclosure by either exposing memory addresses if a user clicks a specially crafted link or by explicitly allowing the use of Secure Sockets Layer (SSL) 2.0. However, in every case an attacker would have no way to force users to click a specially crafted link. An attacker would have to convince users to click the link, typically by way of an enticement in an email or Instant Messenger message.
<a href="#">MS15-089</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow information disclosure if an attacker forces an encrypted Secure Socket Layer (SSL) 2.0 session and uses a man-in-the-middle (MiTM) attack to decrypt parts of the encrypted traffic.
<a href="#">KB3077715</a>	This update supersedes and replaces the update that is described in Microsoft Knowledge Base article 3013410 that was released in December 2014. All additional time zone changes that were released as hotfixes after update 3013410 was released are incorporated in this update.
<a href="#">MS15-080</a>	This security update resolves vulnerabilities in Windows that could allow remote code execution if a user opens a specially crafted document or goes to an untrusted webpage that contains embedded TrueType or OpenType fonts.

Microsoft KnowledgeBase Article ID	Description
<a href="#">MS15-109</a>	This security update resolves vulnerabilities in Windows. These vulnerabilities could allow remote code execution if a user opens a specially crafted toolbar object in Windows or if an attacker convinces a user to view specially crafted content online.
<a href="#">MS15-121</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow spoofing if an attacker performs a man-in-the-middle (MiTM) attack between a client and a legitimate server.
<a href="#">MS15-102</a>	This security update resolves vulnerabilities in Windows that could allow elevation of privilege if an attacker logs on to a system and runs a specially crafted application.
<a href="#">MS15-097</a>	In addition to the changes that are listed for the vulnerabilities that are described in Microsoft Security Bulletin MS15-097, this security bulletin addresses a defense-in-depth update for the secdrv.sys driver, a third-party driver. The update turns off the service for the secdrv.sys driver. This may affect the ability to run some older games.
<a href="#">MS15-097</a>	This security update resolves vulnerabilities in Windows, Microsoft Office, and Microsoft Lync. The most severe of the vulnerabilities could allow remote code execution if a user opens a specially crafted document or goes to an untrusted webpage that contains embedded OpenType fonts.
<a href="#">MS15-119</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker logs on to a computer and runs specially crafted code that exploits the vulnerability.
<a href="#">MS15-109</a>	This security update resolves vulnerabilities in Windows. These vulnerabilities could allow remote code execution if a user opens a specially crafted toolbar object in Windows or if an attacker convinces a user to view specially crafted content online.
<a href="#">KB3097966</a>	Microsoft has released a Microsoft security advisory about this issue for IT professionals. The security advisory contains additional security-related information.
<a href="#">MS15-118</a>	This update resolves vulnerabilities in the Microsoft .NET Framework. The most severe of these vulnerabilities could allow elevation of privilege if an attacker injects a client-side script into a user's browser.
<a href="#">MS15-128</a>	This update resolves vulnerabilities in the Microsoft .NET Framework. The vulnerabilities could allow remote code execution if a user opens a specially crafted document or visits a webpage that contains specially crafted embedded fonts.
<a href="#">MS15-114</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a user opens a specially crafted Journal file. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who have administrative user rights.
<a href="#">MS15-122</a>	This security update resolves a security feature bypass in Windows. An attacker could bypass Kerberos authentication on a computer and decrypt drives that have BitLocker enabled. The bypass can be exploited only if the computer has BitLocker enabled without a PIN or USB key, the computer is domain joined, and the attacker has physical access to the computer.
<a href="#">MS15-117</a>	This security update resolves a vulnerability in Microsoft Windows NDIS. The vulnerability could allow elevation of privilege if an attacker logs on to a system and runs a specially crafted application.
<a href="#">MS15-115</a>	This security update resolves vulnerabilities in Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker convinces a user to open a specially crafted document or to go to an untrusted webpage that contains embedded fonts.

Microsoft KnowledgeBase Article ID	Description
<a href="#">MS15-124</a>	This security update resolves several reported vulnerabilities in Internet Explorer. The most severe of these vulnerabilities could allow remote code execution if a user views a specially crafted webpage in Internet Explorer.
<a href="#">MS15-132</a> <a href="#">KB3108381</a>	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow remote code execution if an attacker accesses a local system and runs a specially crafted application.
<a href="#">MS16-007</a> <a href="#">KB3109560</a> <a href="#">KB3110329</a>	This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker is able to log on to a target system and run a specially crafted application.
<a href="#">MS15-134</a>	This security update resolves vulnerabilities in Microsoft Windows. The more severe of the vulnerabilities could allow remote code execution if Windows Media Center opens a specially crafted Media Center link (.mcl) file that references malicious code. An attacker who successfully exploited this vulnerability could gain the same user rights as the current user. Customers whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.
<a href="#">MS15-130</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a user opens a specially crafted document or visits an untrusted webpage that contains specially crafted fonts.
<a href="#">MS15-128</a>	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow elevation of privilege if an attacker logs on to a targeted system and runs a specially crafted application.
<a href="#">MS15-133</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker logs on to a targeted system and runs a specially crafted application that, by way of a race condition, results in references to memory locations that have already been freed.
<a href="#">KB3112343</a>	This article describes an update that contains some improvements to Windows Update Client in Windows 7 Service Pack 1 (SP1) and Windows Server 2008 R2 SP1.
<a href="#">MS16-013</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a user opens a specially crafted Journal file. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.
<a href="#">MS16-019</a>	This update resolves a vulnerability in the Microsoft .NET Framework. The vulnerability could allow denial of service if an attacker inserts specially crafted XSLT into a client-side XML web part that causes recursive calls on the server.
<a href="#">KB3123479</a>	Microsoft has released a Microsoft security advisory about this issue for IT professionals. The security advisory contains additional security-related information.
<a href="#">MS16-005</a>	This security update resolves vulnerabilities in Microsoft Windows. The more severe of the vulnerabilities could allow remote code execution if a user visits a malicious website.
<a href="#">MS16-001</a>	This security update resolves several reported vulnerabilities in Internet Explorer. The most severe of these vulnerabilities could allow remote code execution if a user views a specially crafted webpage in Internet Explorer.
<a href="#">MS16-016</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker uses the Microsoft Web Distributed Authoring and Versioning (WebDAV) client to send specifically crafted input to a server.



Microsoft KnowledgeBase Article ID	Description
<a href="#">MS16-014</a> <a href="#">KB3126593</a>	This security update resolves vulnerabilities in Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker is able to log on to a target system and run a specially crafted application.
<a href="#">MS16-019</a>	This update resolves a vulnerability in the Microsoft .NET Framework. The vulnerability could allow denial of service if an attacker inserts specially crafted XSLT into a client-side XML web part that causes recursive calls on the server.
<a href="#">MS16-035</a> <a href="#">KB3135988</a>	This update resolves a vulnerability in the Microsoft .NET Framework. The security feature bypass exists in a .NET Framework component that does not properly validate certain elements of a signed XML document.
<a href="#">KB3138612</a>	This article describes an update that contains some improvements to Windows Update Client in Windows 7 Service Pack 1 (SP1) and Windows Server 2008 R2 SP1.
<a href="#">MS16-027</a> <a href="#">KB3138962</a>	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow remote code execution if a user opens specially crafted media content that is hosted on a website.
<a href="#">MS16-033</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker with physical access inserts a specially crafted USB device into the system.
<a href="#">MS16-034</a>	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow elevation of privilege if an attacker logs on to the system and runs a specially crafted application.
<a href="#">MS16-032</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if the Windows Secondary Logon Service fails to properly manage request handles in memory.
<a href="#">MS16-030</a>	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow remote code execution if Windows OLE fails to properly validate user input. An attacker could exploit the vulnerabilities to execute malicious code. However, an attacker must first convince a user to open a specially crafted file or a program from either a webpage or an email message.
<a href="#">MS16-031</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker is able to log on to a target system and run a specially crafted application.
<a href="#">MS16-026</a>	This security update resolves vulnerabilities in Microsoft Windows. The more severe of the vulnerabilities could allow remote code execution if an attacker convinces a user to either open a specially crafted document or visit a webpage that contains specially crafted, embedded OpenType fonts.
<a href="#">MS16-039</a>	This security update resolves vulnerabilities in the Microsoft .NET Framework. The vulnerabilities could allow remote code execution if a user opens a specially crafted document or visits a webpage that contains specially crafted embedded fonts.
<a href="#">MS16-039</a>	This security update resolves vulnerabilities in Microsoft Windows, Microsoft .NET Framework, Microsoft Office, Skype for Business, and Microsoft Lync. The most severe of the vulnerabilities could allow remote code execution if a user opens a specially crafted document or visits a webpage that contains specially crafted embedded fonts.

<b>Microsoft KnowledgeBase Article ID</b>	<b>Description</b>
<a href="#">MS16-044</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if Windows OLE fails to properly validate user input. An attacker could exploit the vulnerability to execute malicious code. However, an attacker must first convince a user to open either a specially crafted file or a program from either a webpage or an email message.
<a href="#">MS16-040</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a user clicks a specially crafted link that could allow an attacker to run malicious code remotely to take control of the user's system. However, in all cases an attacker would have no way to force a user to click a specially crafted link. An attacker would have to convince a user to click the link, typically by way of an enticement in an email or Instant Messenger message.
<a href="#">MS16-047</a>	An elevation of privilege vulnerability exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) remote protocols when they accept authentication levels that do not protect these protocols adequately. The vulnerability is caused by the way the SAM and LSAD remote protocols establish the Remote Procedure Call (RPC) channel. An attacker who successfully exploited this vulnerability could gain access to the SAM database.
<a href="#">KB958488</a>	This article describes an update that consists of Shared Components for Microsoft .NET Framework on Windows 7 and on Windows Server 2008 R2. This update addresses a set of issues of the Microsoft .NET Framework 3.5 Service Pack 1 (SP1).
<a href="#">KB2533552</a>	An update that prevents a "0xc0000034" error message when you try to install Windows 7 SP1, Windows Server 2008 R2 SP1, or Windows Embedded Standard 7 SP1 is available
<b>Microsoft KnowledgeBase Article ID</b>	<b>Description</b>
<a href="#">KB2798162</a>	Update to improve messaging in dialog boxes when you run executable files in Windows.
<a href="#">KB2813430</a>	This software update provides the following improvements for Windows:  Enables administrators to configure domain-joined computers to use the auto update feature for both trusted and disallowed Certificate Trust Lists (CTLs). The computers can use the auto update feature without accessing the Windows Update site.  Enables administrators to configure domain-joined computers to independently select trusted and disallowed CTLs by using the auto update feature.  Enables administrators to examine the set of the root certification authorities (CAs) in the Microsoft Root Certificate Program.
<a href="#">KB2836943</a>	An update for the Microsoft .NET Framework 3.5.1 is available. For more information about the issues that the update resolves, see the "Issues that this update resolves" section.
<a href="#">KB2839894</a>	MS13-050: Vulnerability in Windows print spooler components could allow elevation of privilege: June 11, 2013.
<a href="#">KB2862152</a>	Microsoft security advisory: Vulnerability in IPsec could allow security feature bypass
<a href="#">KB2862330</a>	MS13-081: Description of the security update for USB drivers: October 8, 2013
<a href="#">KB2862335</a>	MS13-081: Description of the security update for USB drivers: October 8, 2013
<a href="#">KB2862973</a>	Microsoft Security Advisory: Update for deprecation of MD5 hashing algorithm for Microsoft root certificate program: August 13, 2013

Microsoft KnowledgeBase Article ID	Description
<a href="#">KB2864202</a> <a href="#">KB2868038</a> <a href="#">KB2884256</a>	MS13-081: Description of the security update for USB drivers: October 8, 2013
<a href="#">KB2868626</a>	MS13-095: Vulnerability in XML digital signatures could allow denial of service: November 12, 2013
<a href="#">KB2871997</a>	Microsoft Security Advisory: Update to improve credentials protection and management: May 13, 2014
<a href="#">KB2887069</a>	MS13-101: Description of the security update for Windows kernel-mode drivers: December 10, 2013
<a href="#">KB2892074</a>	MS13-099: Description of the security update for Windows Script 5.8: December 10, 2013
<a href="#">KB2893294</a>	MS13-098: Vulnerability in Windows could allow remote code execution: December 10, 2013
<a href="#">KB2894844</a>	<p>This security update resolves a vulnerability in the Microsoft .NET Framework 3.5.1 that could allow elevation of privilege on a server system if a user views a specially crafted webpage by using a web browser that can run ASP.NET applications.</p> <p>This security update applies to Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1.</p>
<a href="#">KB2900986</a>	MS13-090: Cumulative security update for ActiveX Kill Bits: November 12, 2013
<a href="#">KB2911501</a>	This update resolves vulnerabilities that could allow elevation of privilege if a user goes to a specially crafted website or a website that contains specially crafted web content.
<a href="#">KB2918614</a>	MS14-049: Description of the security update for Windows Installer Service: August 12, 2014
<a href="#">KB2929733</a>	The first stage of the WER protocol is not SSL encrypted in Windows
<a href="#">KB2931356</a>	MS14-026: Description of the security update for the .NET Framework 3.5.1 on Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1: May 13, 2014
<a href="#">KB2937610</a>	MS14-046: Description of the security update for the .NET Framework 3.5.1 on Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1: August 12, 2014
<a href="#">KB2939576</a>	MS14-033: Description of the security update for MSXML: June 10, 2014
<a href="#">KB2957189</a>	MS14-031: Description of the security update for TCP for Windows: June 10, 2014
<a href="#">KB2957509</a>	MS14-036: Description of the security update for Windows 7, Windows Server 2008 R2, Windows Server 2008, Windows Vista, and Windows Server 2003: June 10, 2014
<a href="#">KB2961072</a>	MS14-040: Description of the security update for an ancillary function driver: July 8, 2014
<a href="#">KB2968294</a>	MS14-057: Description of the security update for the .NET Framework 3.5.1 for Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1: October 14, 2014
<a href="#">KB2972100</a>	MS14-057: Description of the security update for the .NET Framework 3.5.1 for Windows 7 SP1 and Windows Server 2008 R2 SP1: October 14, 2014
<a href="#">KB2972211</a>	MS14-053: Description of the security update for the .NET Framework 3.5.1 for Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1: September 9, 2014
<a href="#">KB2973201</a>	<p>This security update resolves a vulnerability in Windows that could allow elevation of privilege if an attacker uses a vulnerability in a low-integrity process to execute the on-screen keyboard (OSK) and upload a specially crafted program to the target system.</p>

<b>Microsoft KnowledgeBase Article ID</b>	<b>Description</b>
<a href="#">KB2973351</a>	Microsoft Security Advisory: Registry update to improve credentials protection and management for Windows-based systems that have the 2919355 update installed: July 8, 2014
<a href="#">KB2976897</a>	MS14-045: Description of the security update for kernel-mode drivers: August 12, 2014
<a href="#">KB2977292</a>	Microsoft security advisory: Update for Microsoft EAP implementation that enables the use of TLS: October 14, 2014
<a href="#">KB2978120</a>	This update resolves a vulnerability in the Microsoft .NET Framework that could allow elevation of privilege.
<a href="#">KB2978668</a>	MS14-047: Vulnerability in LRPC could allow security feature bypass: August 12, 2014
<a href="#">KB2979570</a>	MS14-057: Description of the security update for the .NET Framework 3.5.1 for Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1: October 14, 2014
<a href="#">KB2984972</a>	This Remote Desktop Protocol (RDP) 7.1 update enables the Remote Desktop Connection client to perform restricted administration logons. It also enables the Remote Desktop Service that is running on an RD host to perform restricted administration.
<a href="#">KB2990214</a>	This article describes an update that enables you to upgrade your computer from Windows 7 Service Pack 1 (SP1) to a later version of Windows.
<a href="#">KB2991963</a>	MS14-078: Description of the security update for IME: November 11, 2014
<a href="#">KB2992611</a>	MS14-066: Vulnerability in SChannel could allow remote code execution: November 11, 2014
<a href="#">KB2993651</a>	MS14-045: Description of the security update for kernel-mode drivers: August 27, 2014
<a href="#">KB3002657</a>	MS15-027: Vulnerability in NETLOGON could allow spoofing: March 10, 2015
<a href="#">KB3003743</a>	MS14-074: Vulnerability in Remote Desktop Protocol could allow security feature bypass: November 11, 2014
<a href="#">KB3004361</a>	MS15-014: Vulnerability in Group Policy could allow security feature bypass: February 10, 2015
<a href="#">KB3004375</a>	Microsoft is announcing the availability of an update for supported editions of Windows 7, Windows Server 2008R2, Windows 8, and Windows Server 2012. This update expands the Audit Process Creation policy to include the command information that is passed to every process. This is a new feature that provides valuable information to help administrators investigate, monitor, and troubleshoot security-related issues on their networks.
<a href="#">KB3005607</a>	MS14-071: Vulnerability in Windows Audio Service could cause Elevation of Privilege: November 11, 2014
<a href="#">KB3006226</a>	MS14-064: Description of the security update for Windows OLE: November 11, 2014
<a href="#">KB3010788</a>	MS14-064: Description of the security update for Windows OLE: November 11, 2014
<a href="#">KB3011780</a>	MS14-068: Vulnerability in Kerberos could allow elevation of privilege: November 18, 2014
<a href="#">KB3014029</a>	MS15-007: Vulnerability in Network Policy Server RADIUS implementation could cause denial of service: January 13, 2015
<a href="#">KB2992611</a>	MS14-066: Vulnerability in SChannel could allow remote code execution: November 11, 2014
<a href="#">KB3019978</a>	MS15-004: Description of the security update for Windows: January 13, 2015

Microsoft KnowledgeBase Article ID	Description
<a href="#">KB3020369</a>	The servicing stack includes the files and resources that are required to service a Windows image. This includes the Package Manager executable, the required servicing libraries, and other resources. The servicing stack is included in all Windows installations.
<a href="#">KB3021674</a>	MS15-003: Vulnerability in Windows User Profile service could allow elevation of privilege: January 13, 2015
<a href="#">KB3022777</a>	MS15-005: Vulnerability in Network Location Awareness service could allow security feature bypass: January 13, 2015
<a href="#">KB3023215</a>	MS15-048: Description of the security update for the .NET Framework 3.5.1 on Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1: May 12, 2015
<a href="#">KB3030377</a>	MS15-028: Vulnerability in Windows Task Scheduler could allow security feature bypass: March 10, 2015
<a href="#">KB3032323</a>	MS15-021: Vulnerabilities in Adobe font driver could allow remote code execution: March 10, 2015
<a href="#">KB3032655</a>	This update resolves vulnerabilities in the Microsoft .NET Framework. These vulnerabilities could allow denial of service (DoS).
<a href="#">KB3033889</a>	MS15-020: Description of the security update for Windows text services: March 10, 2015
<a href="#">KB3033929</a>	Microsoft security advisory: Availability of SHA-2 code signing support for Windows 7 and Windows Server 2008 R2: March 10, 2015
<a href="#">KB3035126</a>	MS15-029: Vulnerability in Windows Photo Decoder component could allow information disclosure: March 10, 2015
<a href="#">KB3035132</a>	MS15-024: Vulnerability in PNG processing could allow information disclosure: March 10, 2015
<a href="#">KB3037574</a>	MS15-041: Description of the security update for the .NET Framework 3.5.1 on Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1: April 14, 2015
<a href="#">KB3039066</a>	MS15-020: Description of the security update for Windows shell: March 10, 2015
<a href="#">KB3042058</a>	Microsoft security advisory: Update to default cipher suite priority order: May 12, 2015
<a href="#">KB3042553</a>	MS15-034: Vulnerability in HTTP.sys could allow remote code execution: April 14, 2015
<a href="#">KB3045171</a>	MS15-044 and MS15-051: Description of the security update for Windows font drivers
<a href="#">KB3045685</a>	This security update resolves vulnerabilities in Windows. These vulnerabilities could allow elevation of privilege if an attacker logs on to the system and runs a specially crafted application. To exploit the vulnerabilities, an attacker would first have to log on to the system. This security update addresses the vulnerabilities by correcting how Windows validates impersonation events.
<a href="#">KB3045999</a>	This security update resolves vulnerabilities in Windows. These vulnerabilities could allow elevation of privilege if an attacker logs on to the system and runs a specially crafted application. To exploit the vulnerabilities, an attacker would first have to log on to the system. This security update addresses the vulnerabilities by correcting how Windows validates impersonation events. For more information about the vulnerabilities, see the "More Information" section.

Microsoft KnowledgeBase Article ID	Description
<a href="#">KB3046017</a>	This security update helps resolve an information disclosure vulnerability in Windows, Internet Explorer, and Microsoft Office. To exploit the vulnerability, an attacker would first have to use another vulnerability in Internet Explorer to run code in the sandboxed process. The attacker could then run Notepad, Visio, PowerPoint, Excel, or Word by using an unsafe command-line parameter to effect information disclosure. To be protected from the vulnerability, customers must apply the updates that are provided in this bulletin and also the update for Internet Explorer that is provided in MS15-079. Similarly, customers who are running an affected Office product must also install the applicable updates that are provided in MS15-081.
<a href="#">KB3046269</a>	This security update resolves a vulnerability in Microsoft Windows. An attacker who successfully exploited the vulnerability could take advantage of a known invalid task to cause Task Scheduler to run a specially crafted application in the context of the System account. An attacker could then do the following: <ul style="list-style-type: none"> <li>• Install programs</li> <li>• View, change, or delete data</li> <li>• Create new accounts that have full user rights</li> </ul>
<a href="#">KB3046306</a>	This security update resolves a vulnerability in Windows that could allow remote code execution if an attacker successfully convinces a user to browse to a specially crafted website, open a specially crafted file, or browse to a working directory that contains a specially crafted Enhanced Metafile (EMF) image file. However, in every case an attacker would have no way to force users to take such actions. An attacker would have to convince users to do this. Typically, the attacker would do this by using enticements in email or instant messaging (IM) messages.
<a href="#">KB3046482</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow security feature bypass if a user clicks a specially crafted link. However, in every case an attacker would have no way to force users to click a specially crafted link. An attacker would have to convince users to click the link, typically by way of an enticement in an email or Instant Messenger message.
<a href="#">KB3055642</a>	This security update resolves a vulnerability in Windows Service Control Manager (SCM). This vulnerability is caused when SCM incorrectly verifies impersonation levels. The vulnerability could allow elevation of privilege if an attacker can first log on to the system and then run a specially crafted application that is designed to increase privileges.
<a href="#">KB3057839</a>	This security update resolves vulnerabilities in Windows. The most severe of these vulnerabilities could allow elevation of privilege if an attacker logs on to the system and runs a specially crafted application. An attacker could then install programs; view, change, or delete data; or create new accounts that have full user rights.
<a href="#">KB3058515</a>	This security update resolves several reported vulnerabilities in Internet Explorer. The most severe of these vulnerabilities could allow remote code execution if a user views a specially crafted webpage in Internet Explorer. To learn more about the vulnerabilities, see Microsoft Security Bulletin MS15-056. Additionally, this security update includes several non-security-related fixes for Internet Explorer. Check out the deployment information.
<a href="#">KB3059317</a>	This security update resolves a vulnerability in Windows that could allow remote code execution if a user clicks a specially crafted link or a link to specially crafted content and then invokes F12 developer tools in Internet Explorer.

Microsoft KnowledgeBase Article ID	Description
<a href="#">KB3060716</a>	<p>This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow elevation of privilege if an attacker logs on to an affected system and runs a specially crafted application or convinces a user to open a specially crafted file that invokes a vulnerable sandboxed application, allowing an attacker to escape the sandbox.</p> <p>This security update is rated Important for all supported releases of Microsoft Windows except Windows 10, which is not affected. For more information, see the Affected Software section.</p>
<a href="#">KB3061518</a>	<p>This security update resolves a vulnerability in Windows. The vulnerability could allow information disclosure when Secure Channel (Schannel) allows the use of a weak Diffie-Hellman ephemeral (DHE) key length of 512 bits in an encrypted Transport Layer Security (TLS) session. Allowing 512-bit DHE keys makes DHE key exchanges weak and vulnerable to various attacks. For an attack to be successful, a server has to support 512-bit DHE key lengths. Windows TLS servers send a default DHE key length of 1,024 bits.</p>
<a href="#">KB3063858</a>	<p>This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if a user visits a network share (or visits a website that points to a network share) that contains a specially crafted file. However, in every case an attacker would be unable to force a user to visit such a network share or website.</p>
<a href="#">KB3071756</a>	<p>This security update resolves a vulnerability in Windows that could allow elevation of privilege if an attacker inserts a malicious USB device into a target system. An attacker could then write a malicious binary to disk and execute the code.</p>
<a href="#">KB3072305</a>	<p>This security update resolves vulnerabilities in the Microsoft .NET Framework and Microsoft Silverlight. These vulnerabilities could allow remote code execution if a user opens a specially crafted document or goes to an untrusted webpage that contains embedded TrueType or OpenType fonts.</p>
<a href="#">KB3072595</a>	<p>This security update resolves a vulnerability in Active Directory Domain Services (AD DS). The vulnerability could allow denial of service if an authenticated attacker creates multiple computer accounts. To exploit this vulnerability an attacker must have valid credentials.</p>
<a href="#">KB3074543</a>	<p>This update resolves vulnerabilities in the Microsoft .NET Framework that could allow elevation of privilege if a user runs a specially crafted .NET Framework application. To learn more about this vulnerability, see Microsoft Security Bulletin MS15-101.</p>
<a href="#">KB3075220</a>	<p>This security update resolves vulnerabilities in Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker first places a specially crafted dynamic link library (DLL) file in the target user's current working directory and then convinces the user to open an RDP file or to launch a program that is designed to load a trusted DLL file but instead loads the attacker's specially crafted DLL file. An attacker who successfully exploited the vulnerabilities could take complete control of an affected system. An attacker could then install programs, could view, change, or delete data, or could create new accounts that have full user rights.</p>
<a href="#">KB3076895</a>	<p>This security update resolves vulnerabilities in Microsoft Windows and Microsoft Office. The vulnerabilities could allow information disclosure by either exposing memory addresses if a user clicks a specially crafted link or by explicitly allowing the use of Secure Sockets Layer (SSL) 2.0. However, in every case an attacker would have no way to force users to click a specially crafted link. An attacker would have to convince users to click the link, typically by way of an enticement in an email or Instant Messenger message.</p>
<a href="#">KB3076949</a>	<p>This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow information disclosure if an attacker forces an encrypted Secure Socket Layer (SSL) 2.0 session and uses a man-in-the-middle (MiTM) attack to decrypt parts of the encrypted traffic.</p>

Microsoft KnowledgeBase Article ID	Description
<a href="#">KB307771</a>	Microsoft has expanded its online services to a non-proprietary platform with the addition of no-charge Microsoft-sponsored NNTP newsgroups on the Internet. Previously, Microsoft-sponsored electronic service forums were limited to users of CompuServe and MSN. With the creation of these newsgroups, users of Microsoft Access can obtain online service support on the Microsoft Support Web site at <a href="http://www.microsoft.com/communities/newsgroups/en-us/default.aspx">http://www.microsoft.com/communities/newsgroups/en-us/default.aspx</a> by using any Internet service provider.
<a href="#">KB3078601</a>	This security update resolves vulnerabilities in Windows that could allow remote code execution if a user opens a specially crafted document or goes to an untrusted webpage that contains embedded TrueType or OpenType fonts.
<a href="#">KB3080446</a>	This security update resolves vulnerabilities in Windows. These vulnerabilities could allow remote code execution if a user opens a specially crafted toolbar object in Windows or if an attacker convinces a user to view specially crafted content online.
<a href="#">KB3084135</a>	This security update resolves vulnerabilities in Windows that could allow elevation of privilege if an attacker logs on to a system and runs a specially crafted application.
<a href="#">KB3086255</a>	In addition to the changes that are listed for the vulnerabilities that are described in Microsoft Security Bulletin MS15-097, this security bulletin addresses a defense-in-depth update for the secdrv.sys driver, a third-party driver. The update turns off the service for the secdrv.sys driver. This may affect the ability to run some older games.
<a href="#">KB3087039</a>	This security update resolves vulnerabilities in Windows, Microsoft Office, and Microsoft Lync. The most severe of the vulnerabilities could allow remote code execution if a user opens a specially crafted document or goes to an untrusted webpage that contains embedded OpenType fonts.
<a href="#">KB3092601</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker logs on to a computer and runs specially crafted code that exploits the vulnerability.
<a href="#">KB3097966</a>	Microsoft has released a Microsoft security advisory about this issue for IT professionals. The security advisory contains additional security-related information.
<a href="#">KB3097989</a>	This update resolves vulnerabilities in the Microsoft .NET Framework. The most severe of these vulnerabilities could allow elevation of privilege if an attacker injects a client-side script into a user's browser.
<a href="#">KB3099862</a>	This update resolves vulnerabilities in the Microsoft .NET Framework. The vulnerabilities could allow remote code execution if a user opens a specially crafted document or visits a webpage that contains specially crafted embedded fonts.
<a href="#">KB3101722</a>	This security update resolves a vulnerability in Microsoft Windows NDIS. The vulnerability could allow elevation of privilege if an attacker logs on to a system and runs a specially crafted application.
<a href="#">KB3108371</a>	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow remote code execution if an attacker accesses a local system and runs a specially crafted application.
<a href="#">KB3108381</a>	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow remote code execution if an attacker accesses a local system and runs a specially crafted application.



Microsoft KnowledgeBase Article ID	Description
<a href="#">KB3108664</a>	This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker is able to log on to a target system and run a specially crafted application.
<a href="#">KB3108670</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a user opens a specially crafted document or visits an untrusted webpage that contains specially crafted fonts.
<a href="#">KB3109094</a>	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow elevation of privilege if an attacker logs on to a targeted system and runs a specially crafted application.
<a href="#">KB3109103</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker logs on to a targeted system and runs a specially crafted application that, by way of a race condition, results in references to memory locations that have already been freed.
<a href="#">KB3109560</a>	This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker is able to log on to a target system and run a specially crafted application.
<a href="#">KB3110329</a>	This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker is able to log on to a target system and run a specially crafted application.
<a href="#">KB3112343</a>	This update enables support for additional upgrade scenarios from Windows 7 to Windows 10, and provides a smoother experience when you have to retry an operating system upgrade because of certain failure conditions. This update also improves the ability of Microsoft to monitor the quality of the upgrade experience.
<a href="#">KB3115858</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a user opens a specially crafted Journal file. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.
<a href="#">KB3122648</a>	This update resolves a vulnerability in the Microsoft .NET Framework. The vulnerability could allow denial of service if an attacker inserts specially crafted XSLT into a client-side XML web part that causes recursive calls on the server.
<a href="#">KB3123479</a>	Microsoft has released a Microsoft security advisory about this issue for IT professionals. The security advisory contains additional security-related information.
<a href="#">KB3124001</a>	This security update resolves vulnerabilities in Microsoft Windows. The more severe of the vulnerabilities could allow remote code execution if a user visits a malicious website.
<a href="#">KB3124275</a>	This security update resolves several reported vulnerabilities in Internet Explorer. The most severe of these vulnerabilities could allow remote code execution if a user views a specially crafted webpage in Internet Explorer.
<a href="#">KB3124280</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker uses the Microsoft Web Distributed Authoring and Versioning (WebDAV) client to send specifically crafted input to a server.
<a href="#">KB3126587</a>	This security update resolves vulnerabilities in Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker is able to log on to a target system and run a specially crafted application.

Microsoft KnowledgeBase Article ID	Description
<a href="#">KB3126593</a>	This security update resolves vulnerabilities in Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker is able to log on to a target system and run a specially crafted application.
<a href="#">KB3127220</a>	This update resolves a vulnerability in the Microsoft .NET Framework. The vulnerability could allow denial of service if an attacker inserts specially crafted XSLT into a client-side XML web part that causes recursive calls on the server.
<a href="#">KB3133043</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could cause denial of service on a Network Policy Server (NPS) if an attacker sends specially crafted username strings to the NPS. This scenario could prevent RADIUS authentication on the NPS.
<a href="#">KB3134214</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker logs on to an affected system and runs a specially crafted application.
<a href="#">KB3135983</a>	This update resolves a vulnerability in the Microsoft .NET Framework. The security feature bypass exists in a .NET Framework component that does not properly validate certain elements of a signed XML document.
<a href="#">KB3135988</a>	This update resolves a vulnerability in the Microsoft .NET Framework. The security feature bypass exists in a .NET Framework component that does not properly validate certain elements of a signed XML document.
<a href="#">KB3138612</a>	This article describes an update that contains some improvements to Windows Update Client in Windows 7 Service Pack 1 (SP1) and Windows Server 2008 R2 SP1. This update has a prerequisite.
<a href="#">KB3138910</a>	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow remote code execution if a user opens specially crafted media content that is hosted on a website.
<a href="#">KB3138962</a>	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow remote code execution if a user opens specially crafted media content that is hosted on a website.
<a href="#">KB3139398</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker with physical access inserts a specially crafted USB device into the system.
<a href="#">KB3139852</a>	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow elevation of privilege if an attacker logs on to the system and runs a specially crafted application.
<a href="#">KB3139914</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if the Windows Secondary Logon Service fails to properly manage request handles in memory.
<a href="#">KB3139940</a>	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow remote code execution if Windows OLE fails to properly validate user input. An attacker could exploit the vulnerabilities to execute malicious code. However, an attacker must first convince a user to open a specially crafted file or a program from either a webpage or an email message.
<a href="#">KB3140410</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker is able to log on to a target system and run a specially crafted application.

Microsoft KnowledgeBase Article ID	Description
<a href="#">KB3140735</a>	This security update resolves vulnerabilities in Microsoft Windows. The more severe of the vulnerabilities could allow remote code execution if an attacker convinces a user to either open a specially crafted document or visit a webpage that contains specially crafted, embedded OpenType fonts.
<a href="#">KB3142042</a>	This security update resolves vulnerabilities in the Microsoft .NET Framework. The vulnerabilities could allow remote code execution if a user opens a specially crafted document or visits a webpage that contains specially crafted embedded fonts.
<a href="#">KB3145739</a>	This security update resolves vulnerabilities in Microsoft Windows, Microsoft .NET Framework, Microsoft Office, Skype for Business, and Microsoft Lync. The most severe of the vulnerabilities could allow remote code execution if a user opens a specially crafted document or visits a webpage that contains specially crafted embedded fonts.
<a href="#">KB3146706</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if Windows OLE fails to properly validate user input. An attacker could exploit the vulnerability to execute malicious code. However, an attacker must first convince a user to open either a specially crafted file or a program from either a webpage or an email message.
<a href="#">KB3146963</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a user clicks a specially crafted link that could allow an attacker to run malicious code remotely to take control of the user's system. However, in all cases an attacker would have no way to force a user to click a specially crafted link. An attacker would have to convince a user to click the link, typically by way of an enticement in an email or Instant Messenger message.
<a href="#">KB3149090</a>	An elevation of privilege vulnerability exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) remote protocols when they accept authentication levels that do not protect these protocols adequately. The vulnerability is caused by the way the SAM and LSAD remote protocols establish the Remote Procedure Call (RPC) channel. An attacker who successfully exploited this vulnerability could gain access to the SAM database.
<a href="#">KB958488</a>	This article describes an update that consists of Shared Components for Microsoft .NET Framework on Windows 7 and on Windows Server 2008 R2. This update addresses a set of issues of the Microsoft .NET Framework 3.5 Service Pack 1 (SP1).
<a href="#">KB2533552</a>	An update that prevents a "0xC0000034" error message when you try to install Windows 7 SP1, Windows Server 2008 R2 SP1, or Windows Embedded Standard 7 SP1 is available

Microsoft KnowledgeBase Article ID	Description
<a href="#">KB_2883200/KB_2894029</a>	The Windows 8.1 and Windows Server 2012 R2 General Availability update rollup is available. This update rollup package provides a set of reliability, performance, and finishing touch improvements to Windows 8.1 and Windows Server 2012 R2. We recommend that you apply this update rollup as part of your regular maintenance routines.
<a href="#">KB2889543</a>	Text is corrupted when it's typed into a webpage that uses Adobe Flash Player after you install security update 2880289.

Microsoft KnowledgeBase Article ID	Description
<a href="#">KB2894179</a>	Computer stops responding in OOBE Wizard stage in Windows 8.1
<a href="#">KB 3119147</a>	<p>Microsoft has released a security advisory for IT professionals about vulnerabilities in Adobe Flash Player in the following web browsers:</p> <ul style="list-style-type: none"> <li>• Internet Explorer in Windows 8, Windows Server 2012, Windows 8.1, Windows Server 2012 R2, Windows 10, and Windows 10 version 1511</li> <li>• Microsoft Edge in Windows 10 and Windows 10 version 1511</li> </ul>
<a href="#">KB 3135782</a>	<p>This security update resolves vulnerabilities in Adobe Flash Player when it is installed on all supported editions of Windows Server 2012, Windows 8.1, Windows Server 2012 R2, Windows RT 8.1, Windows 10, and Windows 10 Version 1511. For more information, see the "Affected Software" section. The update addresses the vulnerabilities in Adobe Flash Player by updating the affected Adobe Flash libraries that are contained in Internet Explorer 10, Internet Explorer 11, and Microsoft Edge.</p>

# 2016 -Windows 2008, 64Bit - Microsoft® Windows Patches Tested with MAXPRO®VMS

Microsoft KnowledgeBase Article ID	Description
<a href="#">KB2534111</a>	"Computer name cannot contain only numbers" error message when you install Windows 7 by using Windows 7 SP1 integrated installation media
<a href="#">KB2803821</a>	MS13-057: Description of the security update for Windows Media Format Runtime 9 and 9.5 (wmvmod.dll), and for Windows Media Player 11 and 12: July 9, 2013
<a href="#">KB2832414</a>	This update resolves a vulnerability in the Microsoft .NET Framework that could allow remote code execution on a client system if a user views a specially crafted webpage by using a web browser that can run XAML Browser Applications (XBAPs).
<a href="#">KB2833946</a>	This update resolves a vulnerability in the Microsoft .NET Framework that could allow remote code execution on a client system if a user views a specially crafted webpage by using a web browser that can run XAML Browser Applications (XBAPs).
<a href="#">KB2834886</a>	This update resolves a vulnerability that could allow remote code execution on a client system if a user opens a specially crafted document or visits a specially crafted webpage that embeds TrueType font files.
<a href="#">KB2835364</a>	This update resolves a vulnerability that could allow remote code execution on a client system if a user opens a specially crafted document or visits a specially crafted webpage that embeds TrueType font files.
<a href="#">KB2840631</a>	This update resolves a vulnerability in the Microsoft .NET Framework that could allow elevation of privilege on a client system if a user views a specially crafted webpage by using a web browser that can run XAML Browser Applications (XBAPs).
<a href="#">KB2844286</a>	This update resolves a vulnerability in the Microsoft .NET Framework that could allow elevation of privilege on a client system if a user views a specially crafted webpage by using a web browser that can run XAML Browser Applications (XBAPs).
<a href="#">KB2845187</a>	MS13-056: Vulnerability in Microsoft DirectShow could allow remote code execution: July 9, 2013
<a href="#">KB2847311</a>	MS13-081: Description of the security update for kernel-mode drivers: October 8, 2013
<a href="#">KB2847927</a>	MS13-058: Vulnerability in Windows Defender could allow elevation of privilege: July 9, 2013
<a href="#">KB2849470</a>	MS13-062: Vulnerability in remote procedure call could allow elevation of privilege: August 13, 2013
<a href="#">KB2855844</a>	MS13-081: Description of the security update for kernel-mode drivers: October 8, 2013
<a href="#">KB2861191</a>	This update resolves vulnerabilities in the Microsoft .NET Framework that could allow remote code execution if a user goes to a website that contains a specially crafted OpenType font (OTF) file by using a browser that can run XBAP applications.
<a href="#">KB2861698</a>	This update resolves a vulnerability in the Microsoft .NET Framework that could allow for denial of service.
<a href="#">KB2861855</a>	Microsoft Security Advisory: Updates to improve Remote Desktop Protocol network-level authentication: August 13, 2013
<a href="#">KB2862152</a>	Microsoft has released a Microsoft security advisory about this issue for IT professionals. The security advisory contains additional security-related information.
<a href="#">KB2862335</a>	MS13-081: Description of the security update for USB drivers: October 8, 2013

Microsoft KnowledgeBase Article ID	Description
<a href="#">KB2862966</a>	An update is available that improves management of weak certificate cryptographic algorithms in Windows
<a href="#">KB2863240</a>	This update resolves a vulnerability in the Microsoft .NET Framework that could allow for denial of service.
<a href="#">KB2864058</a>	MS13-083: Vulnerability in Windows Common Control Library could allow remote code execution: October 8, 2013
<a href="#">KB2864202</a>	MS13-081: Description of the security update for USB drivers: October 8, 2013
<a href="#">KB2868038</a>	MS13-081: Description of the security update for USB drivers: October 8, 2013
<a href="#">KB2868116</a>	This article describes some updates that improve the content in warning messages that you receive when you try to run local executable files in Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows RT, and Windows Server 2012.
<a href="#">KB2868623</a>	MS13-065: Vulnerability in ICMPv6 could allow denial of service: August 13, 2013
<a href="#">KB2868626</a>	MS13-095: Vulnerability in XML digital signatures could allow denial of service: November 12, 2013
<a href="#">KB2868725</a>	Microsoft security advisory: Update for disabling RC4
<a href="#">KB2872339</a>	MS13-077: Vulnerability in Windows Service Control Manager could allow elevation of privilege: September 10, 2013
<a href="#">KB2875783</a>	MS13-093: Vulnerability in Windows ancillary function driver could allow information disclosure: November 12, 2013
<a href="#">KB2876284</a>	MS13-081: Description of the security update for kernel-mode drivers: October 8, 2013
<a href="#">KB2876331</a>	MS13-089: Vulnerability in Windows Graphics Device Interface could allow remote code execution: November 12, 2013
<a href="#">KB2883150</a>	MS13-081: Description of the security update for kernel-mode drivers: October 8, 2013
<a href="#">KB2888505</a>	MS13-088: Cumulative security update for Internet Explorer: November 12, 2013
<a href="#">KB2900986</a>	MS13-090: Cumulative security update for ActiveX Kill Bits: November 12, 2013
<a href="#">KB3046017</a>	This security update helps resolve an information disclosure vulnerability in Windows, Internet Explorer, and Microsoft Office. To exploit the vulnerability, an attacker would first have to use another vulnerability in Internet Explorer to run code in the sandboxed process. The attacker could then run Notepad, Visio, PowerPoint, Excel, or Word by using an unsafe command-line parameter to effect information disclosure. To be protected from the vulnerability, customers must apply the updates that are provided in this bulletin and also the update for Internet Explorer that is provided in MS15-079. Similarly, customers who are running an affected Office product must also install the applicable updates that are provided in MS15-081.
<a href="#">KB3060716</a>	MS15-090: Vulnerabilities in Windows could allow elevation of privilege: August 11, 2015
<a href="#">KB3069114</a>	This security update resolves vulnerabilities in Windows. The more severe of the vulnerabilities could allow remote code execution if a user opens a specially crafted Windows Journal file. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.
<a href="#">KB3071756</a>	This security update resolves a vulnerability in Windows that could allow elevation of privilege if an attacker inserts a malicious USB device into a target system. An attacker could then write a malicious binary to disk and execute the code.

Microsoft KnowledgeBase Article ID	Description
<a href="#">KB3072305</a>	This security update resolves vulnerabilities in the Microsoft .NET Framework and Microsoft Silverlight. These vulnerabilities could allow remote code execution if a user opens a specially crafted document or goes to an untrusted webpage that contains embedded TrueType or OpenType fonts.
<a href="#">KB3074543</a>	MS15-101: Description of the security update for the .NET Framework 3.5.1 on Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1: September 8, 2015
<a href="#">KB3075220</a>	This security update resolves vulnerabilities in Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker first places a specially crafted dynamic link library (DLL) file in the target user's current working directory and then convinces the user to open an RDP file or to launch a program that is designed to load a trusted DLL file but instead loads the attacker's specially crafted DLL file. An attacker who successfully exploited the vulnerabilities could take complete control of an affected system. An attacker could then install programs, could view, change, or delete data, or could create new accounts that have full user rights.
<a href="#">KB3076895</a>	This security update resolves vulnerabilities in Microsoft Windows and Microsoft Office. The vulnerabilities could allow information disclosure by either exposing memory addresses if a user clicks a specially crafted link or by explicitly allowing the use of Secure Sockets Layer (SSL) 2.0. However, in every case an attacker would have no way to force users to click a specially crafted link. An attacker would have to convince users to click the link, typically by way of an enticement in an email or Instant Messenger message.
<a href="#">KB3076949</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow information disclosure if an attacker forces an encrypted Secure Socket Layer (SSL) 2.0 session and uses a man-in-the-middle (MiTM) attack to decrypt parts of the encrypted traffic.
<a href="#">KB3077715</a>	<p>This update supersedes and replaces the update that is described in Microsoft Knowledge Base article 3013410 that was released in December 2014. All additional time zone changes that were released as hotfixes after update 3013410 was released are incorporated in this update.</p> <p>If you have already deployed update 3013410, read the descriptions of the specific time zone changes that are addressed in this article to determine whether you must deploy this update immediately. If no systems are affected directly, you can schedule deployment at the next available opportunity.</p> <p>We recommend that you deploy the most current Windows cumulative time zone update to guarantee the consistency of the time zone database on all systems.</p>
<a href="#">KB3078601</a>	This security update resolves vulnerabilities in Windows that could allow remote code execution if a user opens a specially crafted document or goes to an untrusted webpage that contains embedded TrueType or OpenType fonts.
<a href="#">KB3080446</a>	This security update resolves vulnerabilities in Windows. These vulnerabilities could allow remote code execution if a user opens a specially crafted toolbar object in Windows or if an attacker convinces a user to view specially crafted content online.
<a href="#">KB3083710</a>	This article describes an update that contains some improvements to Windows Update Client in Windows 7 Service Pack 1 (SP1) and Windows Server 2008 R2 SP1. This update is incompatible with Windows Server Update Services (WSUS) servers without the hardening update 2938066.
<a href="#">KB3084135</a>	This security update resolves vulnerabilities in Windows that could allow elevation of privilege if an attacker logs on to a system and runs a specially crafted application.

Microsoft KnowledgeBase Article ID	Description
<a href="#">KB3086255</a>	MS15-097: Description of the security update for the graphics component in Windows: September 8, 2015
<a href="#">KB3087039</a>	This security update resolves vulnerabilities in Windows, Microsoft Office, and Microsoft Lync. The most severe of the vulnerabilities could allow remote code execution if a user opens a specially crafted document or goes to an untrusted webpage that contains embedded OpenType fonts.
<a href="#">KB3087918</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if Windows Media Center opens a specially crafted Media Center link (.mcl) file that references malicious code. An attacker who successfully exploits this vulnerability could gain the same user rights as the current user. Customers whose accounts are configured to have fewer user rights on the system could be less affected than those who operate with administrative user rights.
<a href="#">KB3088195</a>	This security update resolves vulnerabilities in Windows. The more severe of the vulnerabilities could allow elevation of privilege if an attacker logs on to an affected system and runs a specially crafted application.  Note Customers who are using local and remote reporting attestation solutions should review the details of CVE-2015-2552. This is discussed in the Microsoft security bulletin that is mentioned in the following paragraph.
<a href="#">KB3092601</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker logs on to a computer and runs specially crafted code that exploits the vulnerability.
<a href="#">KB3093513</a>	This security update resolves vulnerabilities in Windows. These vulnerabilities could allow remote code execution if a user opens a specially crafted toolbar object in Windows or if an attacker convinces a user to view specially crafted content online
<a href="#">KB3093983</a>	This security update resolves several reported vulnerabilities in Internet Explorer. The most severe of these vulnerabilities could allow remote code execution if a user views a specially crafted webpage in Internet Explorer.
<a href="#">KB3097966</a>	Microsoft has released a Microsoft security advisory about this issue for IT professionals. The security advisory contains additional security-related information.
<a href="#">KB3097989</a>	This update resolves vulnerabilities in the Microsoft .NET Framework. The most severe of these vulnerabilities could allow elevation of privilege if an attacker injects a client-side script into a user's browser.
<a href="#">KB3099862</a>	This update resolves vulnerabilities in the Microsoft .NET Framework. The vulnerabilities could allow remote code execution if a user opens a specially crafted document or visits a webpage that contains specially crafted embedded fonts.
<a href="#">KB3101722</a>	This security update resolves a vulnerability in Microsoft Windows NDIS. The vulnerability could allow elevation of privilege if an attacker logs on to a system and runs a specially crafted application.
<a href="#">KB3108371</a>	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow remote code execution if an attacker accesses a local system and runs a specially crafted application.
<a href="#">KB3108381</a>	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow remote code execution if an attacker accesses a local system and runs a specially crafted application.



Microsoft KnowledgeBase Article ID	Description
<a href="#">KB3108664</a>	This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker is able to log on to a target system and run a specially crafted application.
<a href="#">KB3108669</a>	This security update resolves vulnerabilities in Microsoft Windows. The more severe of the vulnerabilities could allow remote code execution if Windows Media Center opens a specially crafted Media Center link (.mcl) file that references malicious code. An attacker who successfully exploited this vulnerability could gain the same user rights as the current user. Customers whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.
<a href="#">KB3108670</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a user opens a specially crafted document or visits an untrusted webpage that contains specially crafted fonts.
<a href="#">KB3109094</a>	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow elevation of privilege if an attacker logs on to a targeted system and runs a specially crafted application.
<a href="#">KB3109103</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker logs on to a targeted system and runs a specially crafted application that, by way of a race condition, results in references to memory locations that have already been freed.
<a href="#">KB3109560</a>	This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker is able to log on to a target system and run a specially crafted application.
<a href="#">KB3110329</a>	This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker is able to log on to a target system and run a specially crafted application.
<a href="#">KB3112343</a>	This update enables support for additional upgrade scenarios from Windows 7 to Windows 10, and provides a smoother experience when you have to retry an operating system upgrade because of certain failure conditions. This update also improves the ability of Microsoft to monitor the quality of the upgrade experience.
<a href="#">KB3115858</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a user opens a specially crafted Journal file. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.
<a href="#">KB3122648</a>	This update resolves a vulnerability in the Microsoft .NET Framework. The vulnerability could allow denial of service if an attacker inserts specially crafted XSLT into a client-side XML web part that causes recursive calls on the server.
<a href="#">KB3123479</a>	Microsoft has released a Microsoft security advisory about this issue for IT professionals. The security advisory contains additional security-related information.
<a href="#">KB3124275</a>	This security update resolves several reported vulnerabilities in Internet Explorer. The most severe of these vulnerabilities could allow remote code execution if a user views a specially crafted webpage in Internet Explorer.
<a href="#">KB3124280</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker uses the Microsoft Web Distributed Authoring and Versioning (WebDAV) client to send specifically crafted input to a server.

Microsoft KnowledgeBase Article ID	Description
<a href="#">KB3126587</a>	This security update resolves vulnerabilities in Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker is able to log on to a target system and run a specially crafted application.
<a href="#">KB3126593</a>	This security update resolves vulnerabilities in Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker is able to log on to a target system and run a specially crafted application.
<a href="#">KB3127220</a>	This update resolves a vulnerability in the Microsoft .NET Framework. The vulnerability could allow denial of service if an attacker inserts specially crafted XSLT into a client-side XML web part that causes recursive calls on the server.
<a href="#">KB3134214</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker logs on to an affected system and runs a specially crafted application.
<a href="#">KB3135983</a>	This update resolves a vulnerability in the Microsoft .NET Framework. The security feature bypass exists in a .NET Framework component that does not properly validate certain elements of a signed XML document.
<a href="#">KB3135988</a>	This update resolves a vulnerability in the Microsoft .NET Framework. The security feature bypass exists in a .NET Framework component that does not properly validate certain elements of a signed XML document.
<a href="#">KB3138612</a>	This article describes an update that contains some improvements to Windows Update Client in Windows 7 Service Pack 1 (SP1) and Windows Server 2008 R2 SP1.
<a href="#">KB3138910</a>	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow remote code execution if a user opens specially crafted media content that is hosted on a website.
<a href="#">KB3138962</a>	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow remote code execution if a user opens specially crafted media content that is hosted on a website.
<a href="#">KB3139398</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker with physical access inserts a specially crafted USB device into the system.
<a href="#">KB3139852</a>	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow elevation of privilege if an attacker logs on to the system and runs a specially crafted application.
<a href="#">KB3139914</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if the Windows Secondary Logon Service fails to properly manage request handles in memory.
<a href="#">KB3139940</a>	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow remote code execution if Windows OLE fails to properly validate user input. An attacker could exploit the vulnerabilities to execute malicious code. However, an attacker must first convince a user to open a specially crafted file or a program from either a webpage or an email message.
<a href="#">KB3140410</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker is able to log on to a target system and run a specially crafted application.

Microsoft KnowledgeBase Article ID	Description
<a href="#">KB3140735</a>	This security update resolves vulnerabilities in Microsoft Windows. The more severe of the vulnerabilities could allow remote code execution if an attacker convinces a user to either open a specially crafted document or visit a webpage that contains specially crafted, embedded OpenType fonts.
<a href="#">KB3142042</a>	This security update resolves vulnerabilities in the Microsoft .NET Framework. The vulnerabilities could allow remote code execution if a user opens a specially crafted document or visits a webpage that contains specially crafted embedded fonts.
<a href="#">KB3145739</a>	This security update resolves vulnerabilities in Microsoft Windows, Microsoft .NET Framework, Microsoft Office, Skype for Business, and Microsoft Lync. The most severe of the vulnerabilities could allow remote code execution if a user opens a specially crafted document or visits a webpage that contains specially crafted embedded fonts.
<a href="#">KB3146706</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if Windows OLE fails to properly validate user input. An attacker could exploit the vulnerability to execute malicious code. However, an attacker must first convince a user to open either a specially crafted file or a program from either a webpage or an email message.
<a href="#">KB3146963</a>	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a user clicks a specially crafted link that could allow an attacker to run malicious code remotely to take control of the user's system. However, in all cases an attacker would have no way to force a user to click a specially crafted link. An attacker would have to convince a user to click the link, typically by way of an enticement in an email or Instant Messenger message.
<a href="#">KB3149090</a>	An elevation of privilege vulnerability exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) remote protocols when they accept authentication levels that do not protect these protocols adequately. The vulnerability is caused by the way the SAM and LSAD remote protocols establish the Remote Procedure Call (RPC) channel. An attacker who successfully exploited this vulnerability could gain access to the SAM database.
<a href="#">KB958488</a>	This article describes an update that consists of Shared Components for Microsoft .NET Framework on Windows 7 and on Windows Server 2008 R2. This update addresses a set of issues of the Microsoft .NET Framework 3.5 Service Pack 1 (SP1).
<a href="#">KB2533552</a>	An update that prevents a "0xC0000034" error message when you try to install Windows 7 SP1, Windows Server 2008 R2 SP1, or Windows Embedded Standard 7 SP1 is available

# 2016 - Windows 2012 Server R2 - Microsoft® Windows Patches Tested with MAXPRO® VMS

Microsoft KnowledgeBase Article ID	Description
<a href="#">KB2843630</a>	Update helps unmanaged Office 2010 users work with Microsoft RMS in Windows
<a href="#">KB2862152</a>	Microsoft security advisory: Vulnerability in IPsec could allow security feature bypass
<a href="#">KB2868626</a>	MS13-095: Vulnerability in XML digital signatures could allow denial of service: November 12, 2013
<a href="#">KB2876331</a>	MS13-089: Vulnerability in Windows Graphics Device Interface could allow remote code execution: November 12, 2013
<a href="#">KB2883200</a>	Windows 8.1 and Windows Server 2012 R2 General Availability Update Rollup
<a href="#">KB2884101</a>	MS13-080: Description of the security update for Internet Explorer 11 in Windows 8.1 and Windows Server 2012 R2: October 8, 2013
<a href="#">KB2884846</a>	Windows 8.1 and Windows Server 2012 R2 update rollup: October 2013
<a href="#">KB2887595</a>	Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 update rollup: November 2013
<a href="#">KB2892074</a>	MS13-099: Description of the security update for Windows Script 5.8: December 10, 2013
<a href="#">KB2893294</a>	MS13-098: Vulnerability in Windows could allow remote code execution: December 10, 2013
<a href="#">KB2883200</a>	Windows 8.1 and Windows Server 2012 R2 General Availability Update Rollup
<a href="#">KB2894179</a>	Computer stops responding in OOBE Wizard stage in Windows 8.1
<a href="#">KB2887595</a>	Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 update rollup: November 2013
<a href="#">KB2884846</a>	Windows 8.1 and Windows Server 2012 R2 update rollup: October 2013
<a href="#">KB2898871</a>	This update resolves vulnerabilities that could allow elevation of privilege if a user visits a specially crafted website or a website that contains specially crafted web content.
<a href="#">KB2900986</a>	MS13-090: Cumulative security update for ActiveX Kill Bits: November 12, 2013
<a href="#">KB2901128</a>	This update resolves vulnerabilities which could allow elevation of privilege if a user visits a specially crafted website or a website that contains specially crafted web content.
<a href="#">KB2903939</a>	Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 update rollup: December 2013
<a href="#">KB2904266</a>	December 2013 cumulative time zone update for Windows operating systems
<a href="#">KB2906956</a>	"0x80240017" error when you try to install a Windows Store app in Windows RT 8.1, Windows 8.1, or Windows Server 2012 R2
<a href="#">KB2911106</a>	Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 update rollup: January 2014
<a href="#">KB2912390</a>	MS14-007: Vulnerability in Direct2D could allow remote code execution: February 11, 2014
<a href="#">KB2913152</a>	Windows Photo Viewer prints white lines when you use an XPS driver to print photos in Windows
<a href="#">KB2913270</a>	Windows 8.1 Store improvements: January 2014
<a href="#">KB2913760</a>	Drivers and firmware cannot be updated on Windows 8.1-based devices

Microsoft KnowledgeBase Article ID	Description
<a href="#">KB2916036</a>	MS14-005: Vulnerability in Microsoft XML Core Services could allow information disclosure: February 11, 2014
<a href="#">KB2917929</a>	Compatibility update is available for Windows RT 8.1, Windows 8.1 and Windows Server 2012 R2: February 2014
<a href="#">KB2917993</a>	Screen turns black when it rotates from portrait orientation to landscape orientation in Windows
<a href="#">KB2919355</a>	Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 update: April 2014
<a href="#">KB2919394</a>	Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 update rollup: February 2014
<a href="#">KB2922229</a>	MS14-019: Vulnerability in Windows file handling component could allow remote code execution: April 8, 2014
<a href="#">KB2923300</a>	You can access only the Start screen after you press the "Windows logo key+Period (.)" keyboard shortcut three times in Windows 8.1
<a href="#">KB2923528</a>	Application cannot be started after upgrading to Windows 8.1
<a href="#">KB2923768</a>	Update improves OneDrive (formerly SkyDrive) experience in Windows RT 8.1 and Windows 8.1
<a href="#">KB2928193</a>	RRAS BPA rules update for Windows Server 2012 R2
<a href="#">KB2928680</a>	Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 update rollup: March 2014
<a href="#">KB2930275</a>	MS14-015: Vulnerabilities in Windows kernel mode driver could allow elevation of privilege: March 11, 2014
<a href="#">KB2931366</a>	MS14-026: Description of the security update for the .NET Framework 4.5.1 on Windows 8.1, Windows RT 8.1 and Windows Server 2012 R2 for systems that have update 2919355 installed: May 13, 2014
<a href="#">KB2934520</a>	The Microsoft .NET Framework 4.5.2 for Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2
<a href="#">KB2938066</a>	An update to harden Windows Server Update Services
<a href="#">KB2939087</a>	Fix Windows Update errors
<a href="#">KB2954879</a>	Description of the update for .NET Native in Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2
<a href="#">KB2957189</a>	MS14-031: Description of the security update for TCP for Windows: June 10, 2014
<a href="#">KB2961908</a>	Description of the update rollup of revoked noncompliant UEFI modules for systems that do not have the 2919355 update installed: May 13, 2014
<a href="#">KB2962123</a>	MS14-027: Description of the security update for Windows systems that do not have update 2919355 installed: May 13, 2014
<a href="#">KB2967917</a>	July 2014 update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2
<a href="#">KB2973201</a>	MS14-039: Description of the security update for Windows on-screen keyboard: July 8, 2014
<a href="#">KB2973351</a>	Microsoft Security Advisory: Registry update to improve credentials protection and management for Windows-based systems that have the 2919355 update installed: July 8, 2014
<a href="#">KB2975061</a>	May 2014 servicing stack update for Windows 8.1 and Windows Server 2012 R2

<b>Microsoft KnowledgeBase Article ID</b>	<b>Description</b>
<a href="#">KB2976897</a>	MS14-045: Description of the security update for kernel-mode drivers: August 12, 2014
<a href="#">KB2977292</a>	Microsoft security advisory: Update for Microsoft EAP implementation that enables the use of TLS: October 14, 2014
<a href="#">KB2989930</a>	"Not Connected" status for a paired Surface Pen in Bluetooth settings on Surface Pro 3
<a href="#">KB2992611</a>	MS14-066: Vulnerability in SChannel could allow remote code execution: November 11, 2014
<a href="#">KB2993651</a>	MS14-045: Description of the security update for kernel-mode drivers: August 27, 2014

This page is intentionally left blank

## Honeywell Building Technologies – Security Americas (Head Office)

Honeywell Commercial Security

715 Peachtree St. NE

Atlanta, GA 30308

[www.security.honeywell.com/](http://www.security.honeywell.com/)

☎ +1 800 323 4576

## Honeywell Building Technologies – Security Mexico

Mexico: Av. Santa Fe 94, Torre A, Piso 1, Col. Zedec,

CP 0121, CDMX, Mexico.

Colombia: Edificio Punto 99, Carrera 11a.

98-50, Piso 7, Bogota, Colombia.

clarsupport@honeywell.com

☎ 01.800.083.59.25

[www.honeywell.com](http://www.honeywell.com)

## Honeywell Colombia SAS

Carrera 11A # 98-50

Edificio Punto 99, Piso 7, Bogotá DC

Colombia

## Honeywell Building Technologies – Security Middle East/N. Africa

Emaar Business Park, Sheikh Zayed Road

Building No. 2, 2nd floor, 201

Post Office Box 232362

Dubai, United Arab Emirates

☎: +971 44541704

[www.honeywell.com/security/me](http://www.honeywell.com/security/me)

## Honeywell Building Technologies – Security Europe/South Africa

Aston Fields Road, Whitehouse Industrial Estate

Runcorn, WA7 3DL,

United Kingdom

[www.honeywell.com/security/uk](http://www.honeywell.com/security/uk)

☎ 08448 000 235

## Honeywell Building Technologies – Security Northern Europe

Stationsplein Z-W 961,

1117 CE Schiphol-Oost, Netherlands

[www.security.honeywell.com/nl](http://www.security.honeywell.com/nl)

☎ +31 (0) 299 410 200

## Honeywell Building Technologies – Security Deutschland

Johannes-Mauthe-Straße 14 72458 Albstadt, Germany

[www.security.honeywell.de](http://www.security.honeywell.de)

☎ +49 (0) 7431 801-0

## Honeywell Building Technologies – Security France

Immeuble Lavoisier

Parc de Haute Technologie 3-7 rue Georges Besse 92160 Antony, France

[www.security.honeywell.com/fr](http://www.security.honeywell.com/fr)

☎ +33 (0) 1 40 96 20 50

## Honeywell Building Technologies – Security & Fire (Pacific)

Honeywell Ltd. 9 Columbia Way, BAULKHAM HILLS NSW 2153

Visit: [www.honeywellssecurity.com.au](http://www.honeywellssecurity.com.au). Email: hsf.comms.pacific@Honeywell.com

☎ Tech Support: Australia: 1300 220 345, New Zealand: +64 9 623 5050

## Honeywell Building Technologies – Security Italia SpA

Via Achille Grandi 22, 20097 San Donato Milanese (MI), ITALY

[www.security.honeywell.com/it](http://www.security.honeywell.com/it)

## Honeywell Commercial Security - España

Josefa Valcárcel, 24

28027 - Madrid

España

[www.honeywell.com](http://www.honeywell.com)

☎ +34 902 667 800

## Honeywell Building Technologies – Security Россия и СНГ

121059 Moscow, UI, Kiev 7 Russia

[www.security.honeywell.com/ru](http://www.security.honeywell.com/ru)

☎ +7 (495) 797-93-71

## Honeywell Building Technologies – Security Asia Pacific

Building #1, 555 Huanke Road,

Zhang Jiang Hi-Tech Park Pudong New Area,

Shanghai, 201203, China

[www.asia.security.honeywell.com](http://www.asia.security.honeywell.com)

☎ 400 840 2233

## Honeywell Building Technologies – Security and Fire (ASEAN)

Honeywell International Sdn Bhd

Level 25, UOA Corp Tower, Lobby B

Avenue 10, The Vertical, Bangsar South City

59200, Kuala Lumpur, Malaysia

Visit Partner Connect: [www.partnerconnect.honeywell.com](http://www.partnerconnect.honeywell.com)

Email: [buildings.asean@honeywell.com](mailto:buildings.asean@honeywell.com)

## Technical support (Small & Medium Business):

Vietnam: ☎ +84 4 4458 3369

Thailand: ☎ +66 2 0182439

Indonesia: ☎ +62 21 2188 9000

Malaysia: ☎ +60 3 7624 1530

Singapore: ☎ +65 3158 6830

Philippines: ☎ +63 2 231 3380

## Honeywell Home and Building Technologies (India)

HBT India Buildings

Unitech Trade Centre, 5th Floor,

Sector – 43, Block C, Sushant Lok Phase – 1,

Gurgaon – 122002, Haryana, India

Visit Partner Connect: [www.partnerconnect.honeywell.com](http://www.partnerconnect.honeywell.com)

Email: [HBT-IndiaBuildings@honeywell.com](mailto:HBT-IndiaBuildings@honeywell.com)

Toll Free No: 1-800-103-0339

☎ +91 124 4975000

## Honeywell Building Technologies – Security and Fire (Korea)

Honeywell Co., Ltd. (Korea)

5F SangAm IT Tower,

434, Worldcup Buk-ro, Mapo-gu,

Seoul 03922, Korea

Visit: <http://www.honeywell.com>

Email: [info.security@honeywell.com](mailto:info.security@honeywell.com)

Customer support: [HSG-CS-KR@honeywell.com](mailto:HSG-CS-KR@honeywell.com); +82 1522-8779

☎ +82-2-799-6114



Document: 800-19154V9-C\_Microsoft Windows Patches – 10/2019

[www.honeywell.com/security](http://www.honeywell.com/security)  
+1 800 323 4576 (North America only)  
<https://honeywellsystems.com/ss/techsupp/index.html>

[www.honeywell.com/security/uk](http://www.honeywell.com/security/uk)  
+44 (0) 1928 754 028 (Europe only)  
<https://honeywellsystems.com/ss/techsupp/index.html>