Security Notification
SN 2021-06-30 01

30 June 2021

WIN-PAK creates a Windows user with default password

This article contains:

- Summary
- Potential Vulnerability Synopsis
- Affected Products
- Resolution Description
- Appendix: About CVSS

It applies to:

WIN-PAK version listed in the “Affected Products and Versions” section of this notice

To mitigate the risk:

- Follow Resolution Description procedure.

Skills prerequisite:

Knowledge of WIN-PAK system

Ability to use common Windows Tools.

Summary

This security notification informs users of Honeywell WIN-PAK of an identified potential security vulnerability. Honeywell recommends users to follow the process described in the “Mitigating Factors” section to ensure this potential vulnerability is mitigated in any installed and operational system.

Attention: Due to the wide variety of security controls, implementations and interfaces, it is the responsibility of each customer to assess the potential impact within their specific operating environment(s).

Vulnerability Synopsis

WIN-PAK may have a potential vulnerability concerning the Default password used in the creation of Windows User ‘WINPAKUSER’ during WIN-PAK installation.

Default password for windows user ‘WINPAKUSER’:

CVSS Base Score: 8.1 (High)

CVSS Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Affected Products and Versions

The potential vulnerability affects the following product versions:

- WIN-PAK 4.8.5 and earlier versions.

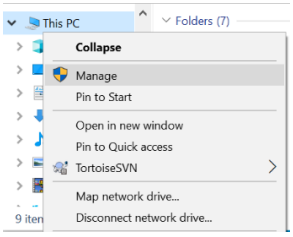
Although an upcoming release of WIN-PAK will automate the mitigation for this issue, until then, we strongly recommend that all customers perform the following mitigation procedure manually in order to protect your local WIN-PAK server machines and network.

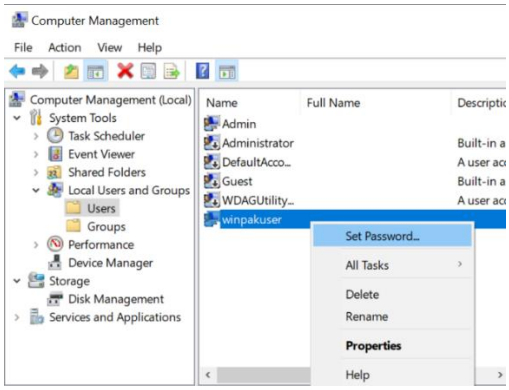
Mitigating Factors

Honeywell recommends that customers running WIN-PAK 4.8.5 and earlier take the following steps:

- This is applicable for customers who have not changed the password of the default created windows user ‘winpakuser’ after the WIN-PAK installation.
- In all the WIN-PAK installed machines, change the password of the windows user ‘WINPAKUSER’ with a unique password and modify the same password in all WIN-PAK services as mentioned below steps.

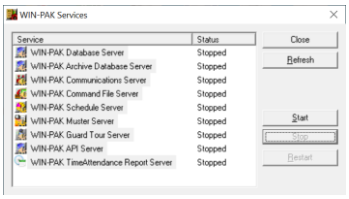
1. Steps to change password of windows user ‘winpakuser’

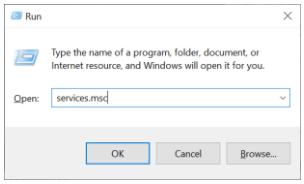


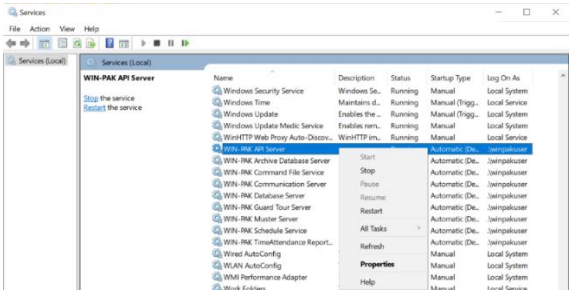


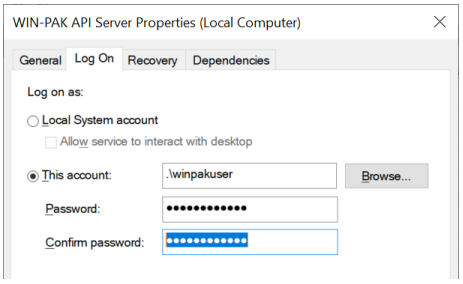
2. Steps to change log on Windows user password of WIN-PAK services

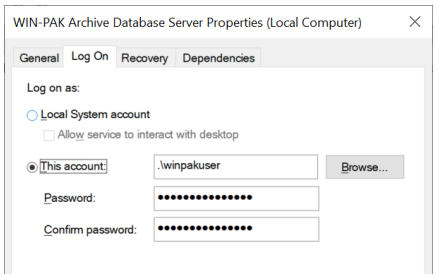
Stop all the WIN-PAK services as below and change the password in WIN-PAK services as below and then start the WIN-PAK services again as below steps.

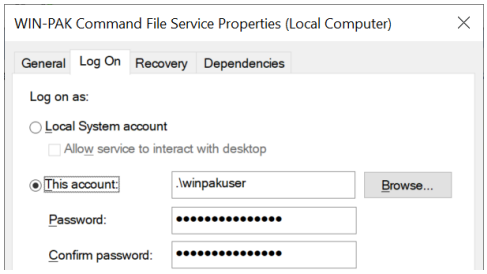


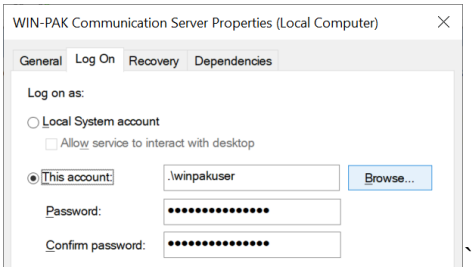


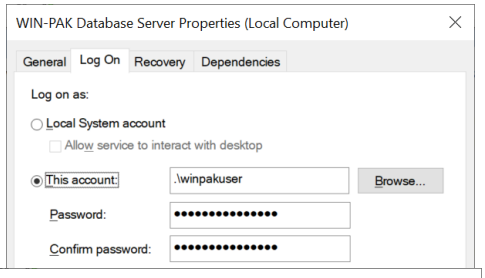


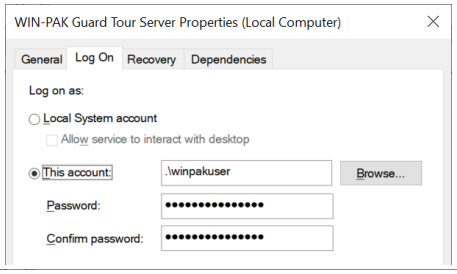

WIN-PAK API Server Properties (Local Computer)
General
Log On
Recovery
Dependencies
Log on as:
Local System account
Allow service to interact with desktop
This account:
.\winpakuser
Browse...
Password:
Confirm password:

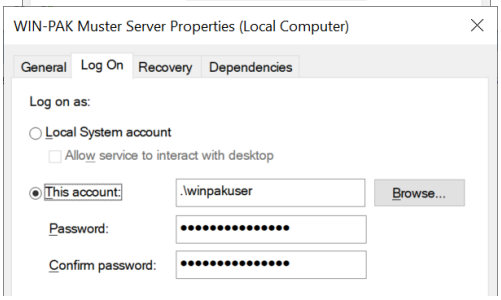

WIN-PAK Archive Database Server Properties (Local Computer)
General
Log On
Recovery
Dependencies
Log on as:
Local System account
Allow service to interact with desktop
This account:
.\winpakuser
Browse...
Password:
Confirm password:

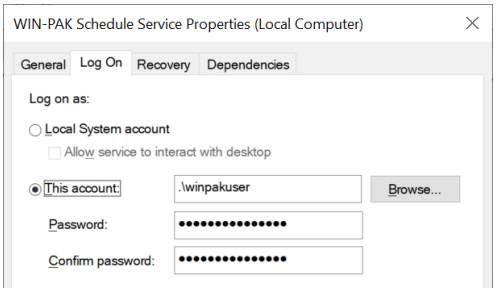

WIN-PAK Command File Service Properties (Local Computer)
General
Log On
Recovery
Dependencies
Log on as:
Local System account
Allow service to interact with desktop
This account:
.\winpakuser
Browse...
Password:
Confirm password:

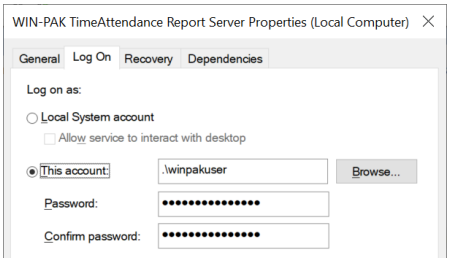

WIN-PAK Communication Server Properties (Local Computer)
General
Log On
Recovery
Dependencies
Log on as:
Local System account
Allow service to interact with desktop
This account:
.\winpakuser
Browse...
Password:
Confirm password:


WIN-PAK Database Server Properties (Local Computer)
General
Log On
Recovery
Dependencies
Log on as:
Local System account
Allow service to interact with desktop
This account:
.\winpakuser
Browse...
Password:
Confirm password:

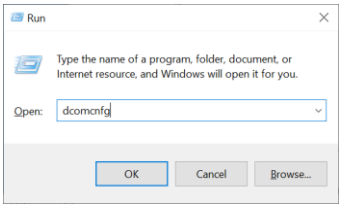

WIN-PAK Guard Tour Server Properties (Local Computer)
General
Log On
Recovery
Dependencies
Log on as:
Local System account
Allow service to interact with desktop
This account:
.\winpakuser
Browse...
Password:
Confirm password:

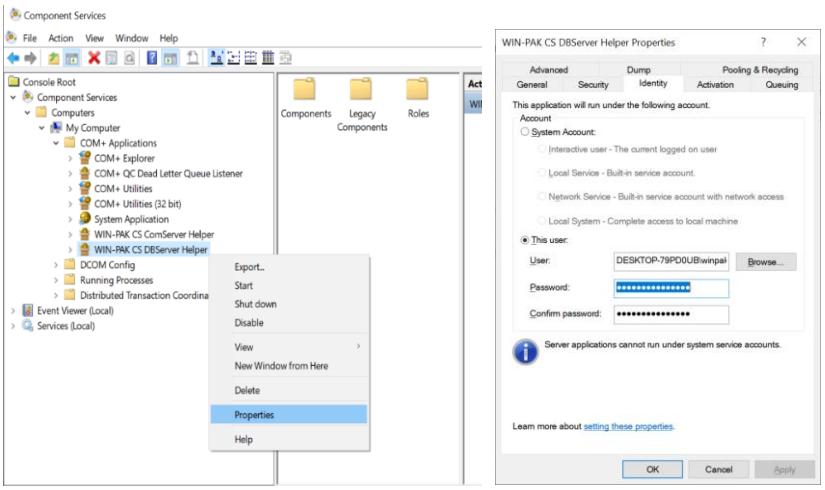

WIN-PAK Muster Server Properties (Local Computer)
General
Log On
Recovery
Dependencies
Log on as:
Local System account
Allow service to interact with desktop
This account:
.\winpakuser
Browse...
Password:
Confirm password:

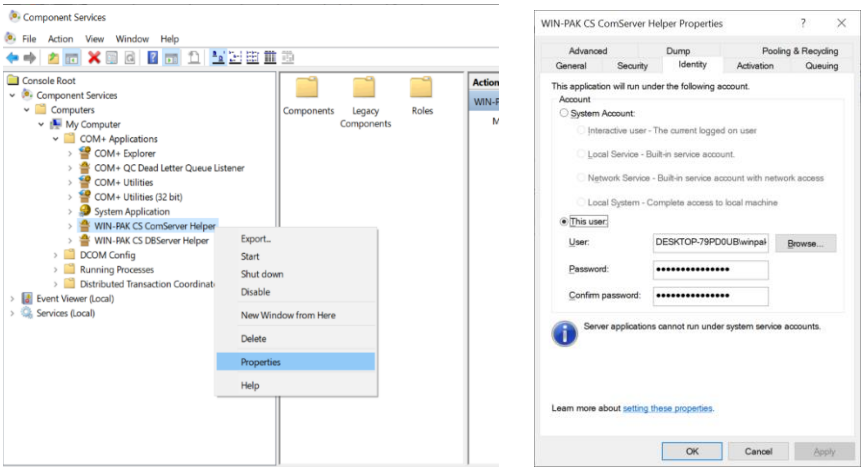

WIN-PAK Schedule Service Properties (Local Computer)
General
Log On
Recovery
Dependencies
Log on as:
Local System account
Allow service to interact with desktop
This account:
.\winpakuser
Browse...
Password:
Confirm password:


WIN-PAK TimeAttendance Report Server Properties (Local Computer)
General
Log On
Recovery
Dependencies
Log on as:
Local System account
Allow service to interact with desktop
This account:
.\winpakuser
Browse...
Password:
Confirm password:

3. Steps to change log on Windows user password of WIN-PAK COM API services







4. Steps to change winpakuser password for WEB

Step 1: Go to the folder "C:\Program Files (x86)\WINPAKPRO\Web\CSACNET" and uncheck the read only & hidden option of 'web.config' file properties

Step 2: Open command prompt (as administrator)

Step 3: Run the below commands cd "C:\Windows\Microsoft.NET\Framework\v2.0.50727" aspnet_regiis -pd "system.web/identity" -app "/csacnet"

Step 4: Open the "C:\Program Files (x86)\WINPAKPRO\Web\CSACNET\web.config" and search with the word 'winpakuser' and update the 'password' field as per the latest (windows user) winpakuser's password and save the 'web.config' file.

Step 5: Run the below command aspnet_regiis -pe "system.web/identity" -app "/csacnet"

Step 6: Check the read only & hidden option of 'web.config' file properties of web.config file.

Resolution Description

Honeywell recommends updating the password of the windows user ‘winpakuser’ in all the WIN-PAK installed machines as mentioned in the Mitigating Factors section above for all affected products listed above.

Attention: This update should be done by qualified personnel.

Contacting Support

For help installing, operating, maintaining, and troubleshooting this product, refer to this document and any other documentation provided. If you still have questions, contact us during business hours (Monday through Friday, excluding holidays).

Notes: Please be ready at the equipment before calling.

Table 1: Technical support

North America
T +1 800 323 4576
W **www.security.honeywell.com/**
Middle East, Turkey & Africa
T +9 714 454 1704
W **www.security.honeywell.com/me**
Europe
T +44 (0) 1928 754 028
W **www.security.honeywell.com/uk**
Asia Pacific
T +400 840 2233
W **www.security.honeywell.com/**

Appendix: About CVSS

The Common Vulnerability Scoring System (CVSS) is an open standard for communicating the characteristics and severity of software vulnerabilities. The Base score represents the intrinsic qualities of a vulnerability. The Temporal score reflects the characteristics of a vulnerability that change over time. The Environmental score is an additional score that can be used by CVSS but is not supplied, as it will differ for each customer.

The severity of the score can be summarized as follows:

Severity Rating	CVSS Score
None	0.0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score. Detailed information about CVSS can be found at http://www.first.org/cvss.

DISCLAIMERS

- CUSTOMERS ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY.
- YOUR USE OF THE INFORMATION ON THIS DOCUMENT OR MATERIALS LINKED FROM THIS DOCUMENT IS AT YOUR OWN RISK.
- HONEYWELL RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME AND WITHOUT NOTICE.
- HONEYWELL PROVIDES THE CVSS SCORES “AS IS” WITHOUT WARRANTY OF ANY KIND. HONEYWELL DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PURPOSE AND MAKES NO EXPRESS WARRANTIES EXCEPT AS MAY BE STATED IN A WRITTEN AGREEMENT WITH AND FOR ITS CUSTOMERS
- IN NO EVENT WILL HONEYWELL BE LIABLE TO ANYONE FOR ANY DIRECT, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES.