Security Notification

INNCOM INNcontrol Reported Security Vulnerability

This article contains:

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

It applies to:

- INNcontrol 3 Versions 3.21 and below

To mitigate the risk:

- Contact INNCOM sales representative or Authorized Systems Integrator to obtain upgrade information.

Skills prerequisite:

- Low attacker skill is required to exploit. Local User access required

---

Summary

This security notification informs users of INNCom INNcontrol 3 (IC3) of a potential security vulnerability. Honeywell recommends that immediate steps be taken to mitigate this potential vulnerability in operational systems.

Attention: Due to the wide variety and uniqueness of security controls, implementations and interfaces, it is the responsibility of each customer to assess the potential impact of vulnerabilities and/or recommendations within their specific operational environment.

Potential Vulnerability Synopsis

The affected product, INNcontrol 3 is a platform to manage guestroom automation and operational efficiency in the hospitality industry. INNcontrol 3 is used for real-time control of energy usage in rooms and to gather and manage information from intelligent INNCOM devices and sensors.

Details of this potential vulnerability are:

Cleartext Storage of Sensitive Information CWE-312

The affected product allows workstation users to escalate application user privileges through the modification of local configuration files.

CVE-2020-6968 has been assigned to this vulnerability.

CVSS Base Score: 6.6 (Medium)

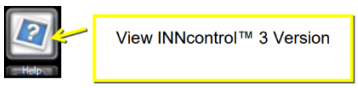
CVSS Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L

Affected Products

The potential vulnerability affects the following product versions:

- INNcontrol 3 Versions 3.21 and below

  The version number of the InnControl software may be checked by clicking the help icon detailed below:



Mitigating Factors

Honeywell recommends that, subject to each customer's individual assessment of the potential impact(s) of the vulnerabilities and/or recommendations on their specific operational building control network environment(s), customers with potentially affected products take the following steps to mitigate the effects of potential vulnerabilities:

- Users are encouraged to contact their INNCOM sales representative or authorized systems integrator to obtain information on upgrading their system(s) to the latest version. Information on contacting INNCOM support is located at https://www.inncom.com/services/support.
- Update the software of potentially impacted systems as per the Security Notification.
- Disable unnecessary accounts and services.
- Restrict system access to authorized personnel only and follow a least privilege approach.
- Apply defense-in-depth strategies.

Appendix: About CVSS

The Common Vulnerability Scoring System (CVSS) is an open standard for communicating the characteristics and severity of computing system 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 Base score has a value ranging from 0 to 10. The Temporal score has the same range and is a modification of the Base score due to current temporary factors.

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 / RECIPIENTS ARE RESPONSIBLE FOR ASSESSING THE IMPACT(S) OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITIES AND / OR RECOMMENDATIONS TO MITIGATE SUCH VULNERABILITIES.
- YOUR USE OF THE INFORMATION IN 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 DAMAGES, INCLUDING BUT NOT LIMITED TO DIRECT, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES, WITH RESPECT TO THE INFORMATION CONTAINED IN, OR ANY ACTIONS / INACTIONS RELATED TO THIS SECURITY NOTIFICATION.