Honeywell

SECURITY NOTICE

SN2026-07-23 #01: AUDIT LOG DISCLOSURE VULNERABILITY IN HONEYWELL S35 SERIES CAMERAS – CVE-2026-17612

This article contains:

It applies to:
Honeywell S35 Series Camera Models listed in the “Affected Products and Versions” section of this notice

Skills prerequisite:
Qualified personnel with Java Script who can perform debug tool with browser.
Ability to use common tools such as analyze network traffic with browser.
Ability to analyze and understand proprietary protocol like HTTP/HTTPS and basic understanding on ONVIF/SOAP.
Ability to write attack scripts and use tools, like curl/python

---

Executive Summary

Honeywell is aware of audit log disclosure vulnerability in S35 Series Camera models.

This vulnerability about audit log disclosure could allow local attacker to potentially exploit this vulnerability, leading to disclosure of sensitive information. This issue has been assigned CVE-2026-17612 and rated with a severity of Medium. Honeywell strongly recommends that users upgrade to the version identified below to resolve the vulnerability.

Vulnerability Synopsis

1. Audit log disclosure vulnerability in Honeywell S35 Series Cameras – CVE-2026-17612

Honeywell

The vulnerability allow a remote attacker to get full administrative audit log without any authentication

CVSS Base Score: CVSS 4.0 / 6.9 (Medium)

CVSS Vector:

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N

CVE Number: CVE-2026-17612

Technical Summary

Honeywell S35 Series Cameras expose audit log information through 2 ONVIF HTTP endpoints without requiring user authentication. While access controls are correctly enforced for other ONVIF log access methods, these endpoints allow unauthenticated users to retrieve the full administrative audit log, resulting in unauthorized access to information intended only for administrators.

Mitigation

See Remediation section below.

For customers who cannot update immediately, the risk and exposure can be reduced by the following measures:

· Isolate their system from the Internet or create additional layers of defense to their system from the Internet by placing the affected hardware behind a firewall or into a DMZ and

· If remote connections to the network are required, consider using a VPN or other means to ensure secure remote connections into the network where the device is located.

Affected Products

Product(s)/ Component(s)	Affected Version	Fixed Version	CVE/Advisory/Update
HON_Honeywell_Series35-3MIPC-HC35WX3RX	HC5.26.1.14.20260207.bin or older version before 2026.02.07	HC5.26.1.16.20260207.bin	**CVE-2026-17612** My Honeywell Buildings University - Download Center
HON_Honeywell_Series35-5MIPC-HC35WX5RX	HC5.26.1.14.20260207.bin or older version before 2026.02.07	HC5.26.1.16.20260207.bin	
HON_Honeywell_Series35-8MIPC(PTZ)-	HC5.26.1.14.20260207.bin or older	HC5.26.1.16.20260207.bin	

HC35WX8RX(HC35WZXRXX)	version before 2026.02.07		
HON_Honeywell_Series35-PinHole-HC35WP5B	HC4.25.1.31.20250828.bin or older version before 2025.08.28	HC5.26.1.16.20260207.bin	

Remediation

Honeywell Product Security strongly recommends affected customers to update their affected products once the update is available.

FAQ

Question:
Do we need to restart camera or an application after applying security fixes or mitigations? If yes, which ones?

Answer:
Camera would be restart after the version updating which would impact existing connected user for their business interruption. After restart, camera would work as normal without any more configuration.

Subscribe to Automated Emails

You may subscribe to the GTAC Knowledge Sharing Mails which provides users with valuable tips & tricks, lessons learned and recommendations on a regular basis.

*(HPS customers only)*Further support required?

If you have any questions concerning this notification, please contact your local Honeywell office or the HPS Technical Support Center. Visit process.honeywell.com and select "Contact Us" for country-specific customer contact numbers.

*(Non-HPS customers)*Further support required?

If you have any questions concerning this notification, please contact PSIRT@Honeywell.com. Visit Product Security (honeywell.com) to view all Honeywell's Security Notices.

Acknowledgement
Honeywell would like to acknowledge Christian Olausson - JebSec for his help in identifying this vulnerability and reporting it to us.

Honeywell

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 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 ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY. CUSTOMER'S FAILURE TO IMPLEMENT THE RECOMMENDED UPDATES OR ACTIONS, INCLUDING WITHOUT LIMITATION, RECOMMENDED PATCHES OR UPDATES TO ANY SOFTWARE OR DEVICE, SHALL BE AT CUSTOMER'S SOLE RISK AND EXPENSE. CUSTOMER SHALL TAKE ALL APPROPRIATE ACTIONS TO SECURE AND SAFEGUARD ITS SYSTEMS AND DATA. HONEYWELL SHALL HAVE NO LIABILITY FOR (I) CUSTOMER'S FAILURE TO IMPLEMENT THE RECOMMENDED UPDATES OR ACTIONS OR (II) CUSTOMER'S FAILURE TO SECURE AND **SAFEGUARD ITS SYSTEMS AND DATA. SUCH FAILURES CAN VOID HONEYWELL'S WARRANTY OBLIGATIONS.**
- 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.