Honeywell

SECURITY NOTICE

SN2026-02-27 #01: VULNERABILITIES IN HIB2PI CCTV CAMERAS (CVE-2026-1670)

This article contains:

It applies to:

- I-HIB2PI-UL cameras
- HDZ322DI and C20WZ2R25 are confirmed as unaffected

Executive Summary

Honeywell has investigated reports concerning CVE-2026-1670 regarding vulnerabilities in certain CCTV camera products. Based on verification with the hardware vendor and an internal security review:

- HDZ322DI and HC20WZ2R25 models are **not vulnerable** to CVE-2026-1670.
- I-HIB2PI-UL was identified as having a vulnerablity. This vulnerability is rated with a severity of Critical and has been published as CWE-306 Missing Authentication for Critical Function. The vulnerability may allow an attacker, locally connected to the network, to change the “forgot password” recovery email address through an unauthenticated API endpoint.

As a mitigation, Honeywell recommends that users follow the guidance in product manuals and configure devices in a protected IT environment, behind a firewall that is not accessible from untrusted networks. A patch is being developed.

Affected Products

Product	CVE	Update
I-HIB2PI-UL (discontinued June 2025)	CVE-2026-1670	Currently no fix is available; a patch is being developed.

Honeywell

Vulnerability Synopsis

1. I-HIB2PI-UL (CVE-2026-1670)

   The affected product is vulnerable to an unauthenticated API endpoint exposure, which may allow an attacker to remotely change the "forgot password" recovery email address.

   CVSS Base Score: 9.8 (Critical)

   CVSS Version 3

   CVE Number: CVE-2026-1670

2. HDZ322DI and HC20WZ2R25 (CVE-2026-1670)

   These were originally referenced as being vulnerable and have been confirmed as not vulnerable to CWE-306 by the hardware vendor and Honeywell internal security reviews.

Mitigation

Honeywell recommends that users follow the guidance in product manuals and configure devices in a protected IT environment, behind a firewall that is not accessible from untrusted networks.

Additional Information

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.

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:

Honeywell

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.