

Security Notification SN 2022-01-26 01

26 Jan 2022

IP PTZ Camera HDZP252DI Command Injection Vulnerability

This article contains:

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

It applies to:

Video products listed in the “Affected Products and Versions” section of this notice

To mitigate the risk:

- Follow Resolution Description procedure.

Skills prerequisite:

Ability to download firmware update.
Ability to follow firmware installation instructions.

Summary

This security notification informs users of Honeywell IP Cameras of an identified potential security vulnerability. Honeywell recommends that 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 a specific operating environment.

Vulnerability Synopsis

1. When controlling this PTZ camera over the default insecure Onvif protocol (i.e., not secured via TLS), the camera may be vulnerable to pan-tilt-zoom command injection. The solution to this secures this interface by using Onvif over TLS 1.2 as the default communications channel.

CVSS Base Score: 6.5 (Medium)

Temporal Score: 5.9 (Medium)

CVSS Vector:

<https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:L/E:P/RL:O/RC:C>

CVE Number:

<https://nvd.nist.gov/vuln/detail/CVE-2021-39363>

Affected Products and Versions

This list shows the models and the minimum firmware version that fixes this vulnerability. If your devices are running firmware versions that are the same or later than shown below, they are not susceptible to this vulnerability.

| Camera Model | Vulnerability fixed from version |
|--------------|--|
| HDZP252DI | HON_Honeywell_Perf4K-PTZ_HDZP252DI_NTSC_V1.000.HW02.8.20211102.bin |

Mitigating Factors

Honeywell recommends that customers with potentially affected products take the following steps to protect themselves:

- Update firmware of vulnerable devices per this security notification;
- 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.

Resolution Description

Honeywell has released firmware update packages for all affected products listed above.

The package can be downloaded from:

<https://mywebtech.honeywell.com/Home>

Attention: This update should be installed by qualified personnel. Access credentials are required to access this site.

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/

Credit

Thanks to Dave Burke and the team at Fathom5 for reporting this potential vulnerability.

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.
- 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 ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, 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.

