Honeywell

Security Notification
SN 2019-09-04 01

IP Camera Unauthenticated Access to Audio Vulnerability

This article contains:

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

It applies to:

IP Camera products listed in the "Affected Products" section of this notice

To mitigate the risk:

- Follow Resolution Description procedure.

Skills prerequisite:

Ability to basic Internet access

Ability to use common tools

Summary

This security notification informs users of Honeywell IP Cameras 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 a specific operating environment.

Vulnerability Synopsis

IP cameras have a potential vulnerability in unauthenticated access to audio streaming over HTTP.

CVSS Base Score: 7.5 (High)

Temporal Score: 6.7 (Medium)

CVSS Vector
https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C

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.

equIP® Series Cameras

Model	Vulnerability fixed from version
* H2W2GR1	1.000.0000.18.20190409
H3W2GR1	1.000.HW00.21.20190812
* H3W2GR1V	1.000.0000.18.20190409
H3W2GR2	1.000.HW00.21.20190812
H3W4GR1	1.000.HW00.21.20190812
* H3W4GR1V	1.000.0000.18.20190409
* H4D8GR1	2.420.HW00.9.20180510
H4L2GR1	1.000.0000.18.20190423
* H4L2GR1V	1.000.0000.18.20190423
H4L6GR2	1.000.HW02.8.20190813
H4LGGR2	1.000.HW04.3.20190813
H4W2GR1	1.000.HW00.21.20190812
* H4W2GR1V	1.000.0000.18.20190409
H4W2GR2	1.000.HW00.21.20190812
H4W4GR1	1.000.HW00.21.20190812
* H4W4GR1V	1.000.0000.18.20190409
* HBD8GR1	2.420.HW00.9.20180510
HBL2GR1	2.420.HW01.33.20190812
* HBL2GR1V	1.000.0000.18.20190423
HBL6GR2	1.000.HW04.3.20190813
HBL6GR2	1.000.HW02.8.20190813
HBW2GR1	1.000.HW00.21.20190812
* HBW2GR1V	1.000.0000.18.20190409
HBW2GR3	1.000.HW00.21.20190812
* HBW2GR3V	1.000.0000.18.20190409
HBW4GR1	1.000.HW00.21.20190812
* HBW4GR1V	1.000.0000.18.20190409
* HCD8G	2.420.HW00.9.20180510
HCL2G	1.000.0000.18.20190423
* HCL2GV	1.000.0000.18.20190423
HCW2G	1.000.HW00.21.20190812
* HCW2GV	1.000.0000.18.20190409
HCW4G	1.000.HW00.21.20190812
* HDZ302D	1.000.0041.20180530
* HDZ302DE	1.000.0041.20180530
* HDZ302DIN	1.000.0041.20180530
* HDZ302DIN-C1	1.000.0041.20180530

* HDZ302DIN-S1	1.000.0041.20180530
* HDZ302LIK	1.000.61.1.20180607
* HDZ302LIW	1.000.61.1.20180607
* HFD6GR1	1.000.HW00.9.20180510
* HFD8GR1	1.000.HW00.9.20180510
HM4L8GR1	1.000.HW02.8.20190813
HMBL8GR1	1.000.HW02.8.20190813

Performance Series Cameras

Model	Vulnerability fixed from version
H4D8PR1	1.000.HW01.3.20190820
HFD5PR1	1.000.HW01.1.20190822
HPW2P1	1.000.HW01.3.20190820
* HDZP304DI	1.000.HW10.5.20190812
* HDZP252DI	1.000.HW02.3.20181109

NOTE: Camera models marked with an asterisk (*****) above may already be running a version of firmware that addresses this issue since it was fixed in a previous release. However, we strongly recommend you download and install the latest firmware which incorporates cyber updates for additional issues not described here.

The updated firmware is available for download on Mywebtech.

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/**	

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 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.