Honeywell

Security Notification
SN 2019-09-13 02

13 September 2019

IP Camera and Recorder Replay Attack 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 use common tools such as Wireshark and analyze network traffic.

Ability to analyze and understand proprietary protocol.

Ability to write attack scripts.

Summary

This security notification informs users of Honeywell IP Cameras and Recorders 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 and Recorders have a potential replay attack vulnerability as a weak authentication method is retained for compatibility with legacy products.

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:H/PR:N/UI:R/S:U/C:H/I:H/A:H/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	1.000.0000.19.20190819
H3W2GR1	1.000.HW00.21.20190812
H3W2GR1V	1.000.0000.19.20190819
H3W2GR2	1.000.HW00.21.20190812
H3W4GR1	1.000.HW00.21.20190812
H3W4GR1V	1.000.0000.19.20190819
H4D8GR1	2.420.HW00.12.20190819
H4L2GR1	2.420.HW01.33.20190812
H4L2GR1V	1.000.0000.19.20190819
H4L6GR2	1.000.HW02.8.20190813
H4W2GR1	1.000.HW00.21.20190812
H4W2GR1V	1.000.0000.19.20190819
H4W2GR2	1.000.HW00.21.20190812
H4W4GR1	1.000.HW00.21.20190812
H4W4GR1V	1.000.0000.19.20190819
HBD8GR1	2.420.HW00.12.20190819
HBL2GR1	2.420.HW01.33.20190812
HBL2GR1V	1.000.0000.19.20190819
HBL6GR2	1.000.HW02.8.20190813
HBW2GR1	1.000.HW00.21.20190812
HBW2GR1V	1.000.0000.19.20190819
HBW2GR3	1.000.HW00.21.20190812
HBW2GR3V	1.000.0000.19.20190819
HBW4GR1	1.000.HW00.21.20190812
HBW4GR1V	1.000.0000.19.20190819
HCD8G	2.420.HW00.12.20190819
HCL2G	2.420.HW01.33.20190812
HCL2GV	1.000.0000.19.20190819
HCPB302	1.000.0040.3.20190820
HCW2G	1.000.HW00.21.20190812
HCW2GV	1.000.0000.19.20190819
HCW4G	1.000.HW00.21.20190812
HDZ302D	1.000.0043.6.20190820
HDZ302DE	1.000.0043.6.20190820
HDZ302DIN	1.000.0043.6.20190820
HDZ302DIN-C1	1.000.0043.6.20190820

HDZ302DIN-S1	1.000.0043.6.20190820
HDZ302LIK	1.000.0062.3.20190816
HDZ302LIW	1.000.0062.3.20190816
HEPB302W01A04	1.000.0040.3.20190820
HEPB302W01A10	1.000.0040.3.20190820
HEPZ302W0	1.000.0039.3.20190820
HFD6GR1	1.000.HW00.12.20190819
HFD8GR1	1.000.HW00.12.20190819
HM4L8GR1	1.000.HW02.8.20190813
HMBL8GR1	1.000.HW02.8.20190813
HSW2G1	2.460.HW00.5.R.20190827
HSW2G1	2.460.HW00.5.R.20190827
HSWB2G1	2.460.HW00.5.R.20190827
HSWB2G1	2.460.HW00.5.R.20190827

Performance Series Cameras

Model	Vulnerability fixed from version
H2W2PC1M	1.000.HW01.3.20190820
H2W2PER3	1.000.HW01.3.20190820
H2W2PRV3	1.000.HW01.1.190813
H2W4PER3	1.000.HW01.3.20190820
H2W4PRV3	1.000.HW01.1.190813
H4D3PRV2	1.000.HW01.1.190814
H4D3PRV3	1.000.HW01.1.190814
H4D8PR1	1.000.HW01.3.20190820
H4W2PER2	1.000.HW01.3.20190820
H4W2PER3	1.000.HW01.3.20190820
H4W2PRV2	1.000.HW01.1.190814
H4W4PER2	1.000.HW01.3.20190820
H4W4PER3	1.000.HW01.3.20190820
H4W4PRV2	1.000.HW01.1.190814
H4W4PRV3	1.000.HW01.1.190813
H4W8PR2	1.000.HW01.3.20190820
HBD2PER1	1.000.HW01.3.20190820
HBD3PR1	1.000.HW01.1.190814
HBD3PR2	1.000.HW01.1.190814
HBD8PR1	1.000.HW01.3.20190820
HBW2PER1	1.000.HW01.3.20190820
HBW2PER2	1.000.HW01.3.20190820
HBW2PR1	1.000.HW01.1.190813

HBW2PR2	1.000.HW01.1.190814
HBW4PER1	1.000.HW01.3.20190820
HBW4PER2	1.000.HW01.3.20190820
HBW4PR1	1.000.HW01.1.190813
HBW4PR2	1.000.HW01.1.190814
HBW8PR2	1.000.HW01.3.20190820
HDZP252DI	1.000.HW02.4.20190813
HDZP304DI	1.000.HW10.5.20190812
HED2PER3	1.000.HW01.3.20190820
HED3PR3	1.000.HW01.1.190814
HED8PR1	1.000.HW01.3.20190820
HEW2PER2	1.000.HW01.3.20190820
HEW2PER3	1.000.HW01.3.20190820
HEW2PR1	1.000.HW01.1.190813
HEW2PR2	1.000.HW01.1.190814
HEW2PRW1	1.000.HW01.1.190813
HEW4PER2	1.000.HW01.3.20190820
HEW4PER2B	1.000.HW01.3.20190820
HEW4PER3	1.000.HW01.3.20190820
HEW4PER3B	1.000.HW01.3.20190820
HEW4PR2	1.000.HW01.1.190814
HEW4PR3	1.000.HW01.1.190813
HEW4PRW3	1.000.HW01.1.190813
HFD5PR1	1.000.HW01.1.20190822
HPW2P1	1.000.HW01.3.20190820

Recorders

Model	Vulnerability fixed from version
HEN04102	2.000.HW00.0.R.20190823
HEN04112	2.000.HW00.0.R.20190823
HEN04122	2.000.HW00.0.R.20190823
HEN08102	2.000.HW00.0.R.20190823
HEN08112	2.000.HW00.0.R.20190823
HEN08122	2.000.HW00.0.R.20190823
HEN08142	2.000.HW00.0.R.20190823
HEN08162	2.000.HW00.0.R.20190823
HEN16102	2.000.HW00.0.R.20190823
HEN16122	2.000.HW00.0.R.20190823
HEN16142	2.000.HW00.0.R.20190823
HEN16162	2.000.HW00.0.R.20190823
HEN04103	3.215.00HW001.2.20190821

HEN04113	3.215.00HW001.2.20190821
HEN04123	3.215.00HW001.2.20190821
HEN08103	3.215.00HW001.2.20190821
HEN08113	3.215.00HW001.2.20190821
HEN08123	3.215.00HW001.2.20190821
HEN08143	3.215.00HW001.2.20190821
HEN16103	3.215.00HW001.2.20190821
HEN16123	3.215.00HW001.2.20190821
HEN16143	3.215.00HW001.2.20190821
HEN16163	3.215.00HW001.2.20190821
HEN04103L	3.215.00HW001.2.20190821
HEN08103L	3.215.00HW001.2.20190821
HEN16103L	3.215.00HW001.2.20190821
HEN32103L	3.215.00HW001.2.20190821
HEN08104	3.215.00HW002.2.20190829
HEN08144	3.215.00HW002.2.20190829
HEN081124	3.215.00HW002.2.20190829
HEN16104	3.215.00HW002.2.20190829
HEN16144	3.215.00HW002.2.20190829
HEN16184	3.215.00HW002.2.20190829
HEN32104	3.215.00HW002.2.20190829
HEN321124	3.215.00HW002.2.20190829
HEN16204	3.215.00HW002.2.20190829
HEN16284	3.215.00HW002.2.20190829
HEN162244	3.215.00HW002.2.20190829
HEN32204	3.215.00HW002.2.20190829
HEN32284	3.215.00HW002.2.20190829
HEN322164	3.215.00HW002.2.20190829
HEN64204	3.215.00HW002.2.20190829
HEN642164	3.215.00HW002.2.20190829
HEN16304	3.215.00HW002.2.20190829
HEN16384	3.215.00HW002.2.20190829
HEN32304	3.215.00HW002.2.20190829
HEN32384	3.215.00HW002.2.20190829
HEN323164	3.215.00HW002.2.20190829
HEN64304	3.215.00HW002.2.20190829
HEN643164	3.215.00HW002.2.20190829
HEN643324	3.215.00HW002.2.20190829
HEN643484	3.215.00HW002.2.20190829
HRHT4040	1.000.00HW001.2.190822

HRHT4041	1.000.00HW001.2.190822
HRHT4042	1.000.00HW001.2.190822
HRHT4080	1.000.00HW001.2.190822
HRHT4082	1.000.00HW001.2.190822
HRHT4084	1.000.00HW001.2.190822
HRHT4160	1.000.00HW001.2.190822
HRHT4162	1.000.00HW001.2.190822
HRHT4164	1.000.00HW001.2.190822
HRHT4166	1.000.00HW001.2.190822
HRHT41612	1.000.00HW001.2.190822
HRHQ1040	1.000.00HW001.1.190822
HRHQ1040L	1.000.00HW001.1.190822
HRHQ1041	1.000.00HW001.1.190822
HRHQ1080	1.000.00HW001.1.190822
HRHQ1080L	1.000.00HW001.1.190822
HRHQ1081	1.000.00HW001.1.190822
HRHQ1082	1.000.00HW001.1.190822
HRHQ1160	1.000.00HW001.1.190822
HRHQ1161	1.000.00HW001.1.190822
HRHQ1162	1.000.00HW001.1.190822
HRHQ1164	1.000.00HW001.1.190822

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.