Honeywell

Security Notification
SN 2023-08-02 01

Sep 12, 2023

PM23/43 Printer Vulnerabilities

This article contains:

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

It applies to:

"Affected Products and Versions" section of this notice

To mitigate the risk:

- Follow Resolution Description procedure.

Skills prerequisite:

Device/Printer administration, IT administrator

Summary

A critical severity vulnerability (CVE-2023-3711, CVSSv3 10.0) impacting multiple versions of the PM23/43 printer firmware was discovered.

> **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

The session ID generated by the web application of the PM23/43 is insecure and could be guessed by an attacker. The attacker can potentially impersonate a particular printer web page session, using a complex method to predict/guess the session ID.

CVSS Base Score:	[7.5] ([High])
Temporal Score:	[6.4] ([Medium])

CVSS Vector

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:L/A:L

Affected Products

The potential vulnerability affects the following product versions:

- PM23/43 series of mid-range industrial printers versions before P10.19.050006

Mitigating Factors

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

Update to the latest available firmware version of the respective printers to version MR19.5 (e.g. P10.19.050006) or later.
Disable web access to the printers if firmware update option is not available immediately.

Resolution Description

Honeywell has released an updated firmware version P10.19.050006 for PM23/43 printers.

Credit

Honeywell thanks Siemens and Jinqi Lai for reporting this 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 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.