Honeywell

Security Notification
SN 2017-03-14 01

March 14, 2017

Intermec PM43 Industrial Printers local root with Busybox jailbreak resulting in privilege elevation

This article contains:

It applies to:

PM23, PM42, PM43, PC23, PC43, PD43 and PC42 printers with versions prior to February 2017

To mitigate the risk:

- Follow Resolution Description procedure.

Skills prerequisite:

Linux Administrator

Summary

This security notification informs users of Intermec PM23, PM42, PM43, PC23, PC43, PD43 and PC42 printers of a potential software vulnerability that has been identified. Honeywell recommends that immediate steps be taken 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.

Potential Vulnerability Synopsis

1. Improper permissions setting on the affected printers allows privilege escalation

   CVSS Base Score: 7.5 (CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H) (HIGH)

   CVSS Vector
   http://www.first.org/cvss/calculator/3.0#CVSS:3.0/[vector].

Affected Products

The potential vulnerability affects the following product versions:

- PM23, PM42, PM43, PC23, PC43, PD43 and PC42 printers with versions prior to March 2017

An attacker may be able to exploit a flaw in the printer to perform actions such as attacking or compromising computers with which the printer is able to communicate.

Mitigating Factors

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

- Update firmware of vulnerable instruments as per the security notification
- Always use passwords on installations of printer to prevent unauthorized access
- Allow only trained and trusted persons to have physical access to their system, including devices that have connection to the system though the Ethernet port
- 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
- 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. A VPN is available for use on the printer

Resolution Description

Honeywell has released firmware update package v11.1 (for PM43, PM23 printers: P10.11.013310) and v12.1 (for all others: x10.12.013309).

The package can be downloaded from hsmftp.honeywell.com or by contacting Honeywell Technical Support and asking about Security Notification SN 2017-03-14 01 (this notification).

General release will be available in our next regular firmware release, currently scheduled for July 2017.

Attention: This update should be installed by qualified personnel

Prerequisites

- Ensure you have a backup of any customer-installed files on your printer before installing this update.

To install the update on client printer:

- Contact Honeywell Technical Support (HSMNAsupport@honeywell.com) for assistance in obtaining the update appropriate to your specific printer model. Alternatively, download the update from https://hsmftp.honeywell.com by navigating to your printer's model number.
- Install update according to instructions found in the printer's User Guide. User Guides for your specific printer model may be obtained from the product pages on the Honeywell web site (http://honeywellaidc.com). If distributing the software update via a Mobile Device Manager (MDM), consult the applicable user documentation for instructions.
- Your device will reboot so assure that you have properly saved your settings/data in case of any problems.

Credit

Thanks to Mr Jean-Marie Bourbon 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 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.