Honeywell

Security Notification
SN 2024-03-08 01

Honeywell MPA2 Web Application XSS vulnerability

This article contains:

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

It applies to:

MPA2 with firmware version prior to R1.00.08.05

To mitigate the risk:

- Follow Resolution Description procedure.

Skills prerequisite:

Qualified personnel with MPA2 Admin credentials

Summary

This security notification informs users of MPA2 of a software vulnerability that has been identified. Honeywell recommends that immediate steps be taken to ensure this vulnerability is mitigated in any installed and operational system.

Vulnerability Synopsis

1. XSS / Arbitrary Code Injection in Honeywell MPA2 - Web Application
   Cross-site scripting (also known as XSS) is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application. Code injected into a vulnerable application can exfiltrate data or install malware on the user's machine. Attackers can spoof / masquerade as authorized users via session cookies, allowing them to perform any action allowed by the user account, redirect / hijack MPA2 web server responses, completely.

   CVSS Base Score: 8.1 (High)

   Temporal Score: 7.5 (High)

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

   CVE Number
   https://nvd.nist.gov/vuln/detail/CVE-2023-1841

Affected Products

The vulnerability affects the following product versions:
- MPA2 with firmware prior to version R1.00.08.05

Mitigating Factors

Honeywell recommends that customers with affected products take Update firmware of vulnerable devices as per this security notification.

Resolution Description

Honeywell released a firmware update package **MPA2 firmware R1.00.08.05** that addressed this issue. That **MPA2 firmware R1.00.08.05** that version and all later versions correct the reported vulnerability.

The latest firmware can be downloaded from My Honeywell Buildings University. Click on "Download Center" at the top of the page, select "+ Access Control", click on "MPA®", select "+ MPA2 | MPA4 (MPA2C3 | MKPA2C3-4) - Current", then click on "+ Firmware" and click the download icon for the latest version (⬇).
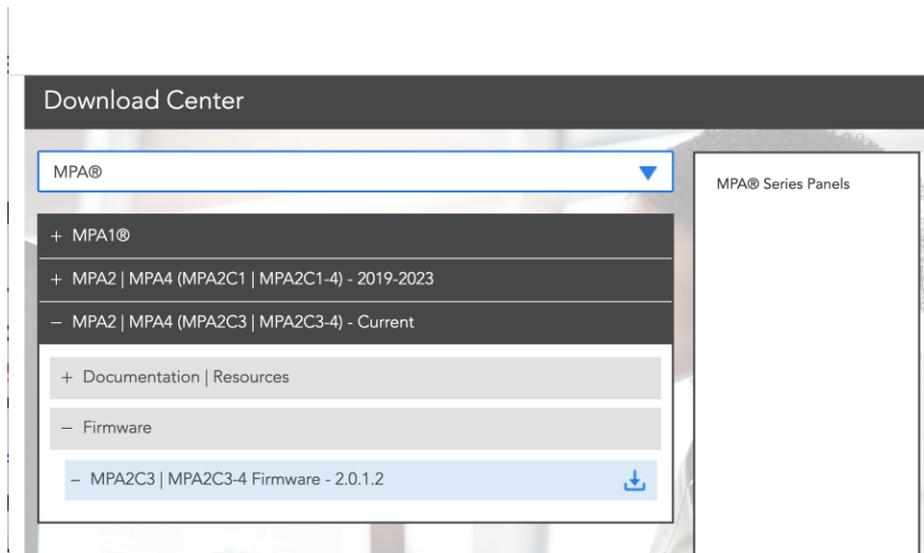
Please refer the MPA2 User Guide for detailed firmware upgrade description.

Firmware can also be upgraded through MaxProCloud for MPC connected MPA2 panels.

> **Attention:** This update should be installed by qualified personnel.

Prerequisites

- **WEB mode**
    - Host machine with Chrome browser with MPA2 web login admin account
- **WIN-PAK mode**
    - Windows host machine with WIN-PAK installed with admin account.
- **MPC mode**
    - MPC admin account

To install the update on MPA2 panel:

1   Firmware Upgrade via web mode
    1. Download the firmware image from - My Honeywell Buildings University as described above.

2. Navigate to the web server Panel Configuration > Advanced > File Management > Upload (To Panel).
3. Under Download click Browse to locate the latest App file.
4. Select the file and click Download. Click OK to continue. Once the "Download to primary panel complete; now processing the image" message pops up, click OK again.
5. You will see the "Download to primary panel complete; now processing the image" message once again. Click OK to continue. This time a reboot will be triggered. It will take approximately 10 to 15 minutes for the Application to complete the installation.

2   Firmware Upgrade via WIN-PAK mode
    1. Download image from - My Honeywell Buildings University.
    2. Copy the downloaded firmware to C:\Program Files\WINPAKPRO\Firmware\releases.
    3. Navigate to Operations \ Control Map and right click on the MPA Primary panel to download.
    4. You can download the firmware only if you have logged on with admin privileges.

3   Firmware Upgrade via MPC
    1. Login to the MPC account using user credentials.
    2. Navigate to Firmware upgrade page.
    3. Select the device and the latest firmware version (R1.00.08.05 or later) to upgrade. It will take approximately 20 minutes for the application to complete the install.

[Warnings]

Please make sure power supply to the MPA2 panel is not interrupted during the upgrade process.
- Do not disconnect the power adaptor if MPA2 panel is powered through power adaptor.
- Do not switch off / restart the router if MPA2 panel is powered through PoE.

Credit

Honeywell thanks Ken Pyle from CYBIR (kp@cybir.com) 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.