Eaton Vulnerability Advisory

ETN-VA-2021-1001c: Eaton Intelligent Power Manager Infrastructure

Date	Overall Risk	CVSS v3.1
02/04/2022	Medium	5.7

Overview

Eaton has been made aware of security vulnerabilities in its Intelligent Power Manager Infrastructure (IPM Infrastructure) software.

Embedded within an Eaton Intelligent Power Controller, the IPM Infrastructure software provided data center managers with an easy to use and simple to deploy infrastructure monitoring solution. The product is now approaching End-of-Life and is being replaced by - the IPM Monitor Edition

Here are the reported vulnerabilities, and the mitigation.

CVE-2021-23284: Score 5.7

Stored Cross-site Scripting

CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:H/E:F/RL:O/RC:C/CR:L/IR:L/AR:H/MAV:A/MPR:H/MUI:R/MS:C/MC:L/MI:L/MA:H

CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Type 2: Stored XSS (or Persistent)

Eaton Intelligent Power Manager Infrastructure (IPM Infrastructure) all versions including 1.5.0plus205 are vulnerable to stored Cross site scripting. The vulnerability exists due to insufficient validation of input from certain resources by the IPM Infrastructure software. The attacker would need access to the local Subnet and an administrator interaction to compromise the system.

CVE-2021-23285: Score 3.1

Reflected Cross-site Scripting

CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:L/I:L/A:N/E:F/RL:O/CR:L/IR:L/AR:H/MAV:A/MPR:H/MA:L

CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Eaton Intelligent Power Manager Infrastructure (IPM Infrastructure) all versions including 1.5.0plus205 are vulnerable to reflected Cross-site Scripting vulnerability. The vulnerability exists due to insufficient validation of input from certain resources by the IPM Infrastructure software. The attacker would need access to the local Subnet and an administrator interaction to compromise the system.

Eaton Vulnerability Advisory

CVE-2021-23286 : Score 5.4

CSV Formula Injection

CVSS:3.1/AV:A/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:H/E:F/RL:U/CR:L/IR:L/AR:H/MAV:A/MPR:H/MA:H

CWE-1236: Improper Neutralization of Formula Elements in a CSV File

Eaton Intelligent Power Manager Infrastructure (IPM Infrastructure) all versions including 1.5.0plus205 are vulnerable to CSV Formula Injection. The vulnerability exists due to improper sanitization of imported CSV files. The attacker would need access to the local Subnet and an administrator interaction to compromise the system.

Affected Product(s) and Version(s)

Here is the list of affected products –

- Eaton Intelligent Power Manager Infrastructure (IPM Infrastructure)– all versions including 1.5.0plus205

Mitigation

Mitigation

The product has reached its End Of Life, the notification has been posted at: Lifecycle Notification.

The transition to IPM Monitor Edition is in progress. Refer the Product page for further details.

Until the transition is complete, Eaton recommends that the below guidelines should be followed.

To prevent the exploitation of the issues and safeguard the software from malicious entities, ensure access to the system is provided to the known users and the credentials are secured.

General Security Best Practices

- Restrict exposure to external networks for all control system devices and/or systems and ensure that they are not directly accessible from the open Internet.
- Deploy control system networks and remote devices behind barrier devices (e.g. firewalls, data diodes) and isolate them from business networks.
- Remote access to control system networks should be made available on a strict need-to-use basis. Remote access should use secure methods, such as Virtual Private Networks (VPNs), updated to the most current version available.
- Regularly update/patch software/applications to latest versions available, as applicable.
- Enable audit logs on all devices and applications.
- Disable/deactivate unused communication channels, TCP/UDP ports and services (e.g., SNMP, FTP, BootP, DHCP, etc.) on networked devices.
- Create security zones for devices with common security requirements using barrier devices (e.g. firewalls, data diodes).

- Change default passwords following initial startup. Use complex secure passwords or passphrases.
- Perform regular security assessments and risk analysis of networked control systems.

For more details on cybersecurity best practices and leverage Eaton's Cybersecurity as a Service, please consult the following –

- Eaton offers a suite of cybersecurity assessment and life-cycle management services to help identify vulnerabilities and secure your operational technology network. These services can help you complete the recommended remediation and mitigation actions and strengthen your overall network security. More information about these services are available at www.eaton.com/cybersecurityservices. If you need immediate support, please call +1-800-498-2678 to connect with a representative.
- Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN)
- Cybersecurity Best Practices Checklist Reminder (WP910003EN)

Acknowledgement

Eaton thanks the below organization and individuals for their coordinated support on the security vulnerabilities: -

- CVE-2021-23284 – Micheal Heinzl via ICS-Cert
- CVE-2021-23285 – Micheal Heinzl via ICS-Cert
- CVE-2021-23286 – Micheal Heinzl via ICS-Cert

Additional Support and Information

For additional information, including a list of vulnerabilities that have been reported on our products and how to address them, please visit our Cybersecurity web site www.eaton.com/cybersecurity, or contact us at PSIRT@eaton.com.

Legal Disclaimer:

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, INFORMATION PROVIDED IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. EATON, ITS AFFILIATES, SUBSIDIARIES, AND AUTHORIZED REPRESENTATIVES HEREBY DISCLAIM ALL WARRANTIES AND CONDITIONS OF ANY KIND EITHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, INCLUDING, BUT WITHOUT LIMITATION, ANY IMPLIED WARRANTIES AND/OR CONDITIONS OF SECURITY, COMPLETENESS, TIMELINESS, ACCURACY, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR LIMITATIONS, SO THE ABOVE LIMITATIONS MAY NOT APPLY. TO THE EXTENT PERMITTED BY LAW, IN NO EVENT WILL EATON OR ITS AFFILIATES, OFFICERS, DIRECTORS, AND/OR EMPLOYEES, BE LIABLE FOR ANY LOSS OR DAMAGE OF ANY KIND WHATSOEVER, INCLUDING, BUT NOT LIMITED TO, ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, STATUTORY, PUNITIVE, ACTUAL, LIQUIDATED, EXEMPLARY, CONSEQUENTIAL OR OTHER DAMAGES, EVEN IF EATON HAS BEEN ADVISED OF THE POSSIBILITY OF

SUCH DAMAGES. THE USE OF THIS NOTIFICATION, INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED TO IT ARE AT YOUR OWN RISK. EATON RESERVES THE RIGHT TO UPDATE OR CHANGE THIS NOTIFICATION AT ANY TIME AND AT ITS SOLE DISCRETION.

About Eaton:

Eaton is a power management company. We provide energy-efficient solutions that help our customers effectively manage electrical, hydraulic and mechanical power more efficiently, safely and sustainably. Eaton is dedicated to improving the quality of life and the environment through the use of power management technologies and services. Eaton has approximately 100,000 employees and sells products to customers in more than 175 countries.

Revision Control:

Date	Version	Notes
02/04/2022	v1.0	Initial Public Advisory

Office:

Eaton, 1000 Eaton Boulevard

Cleveland, OH 44122, United States

Eaton.com