Eaton Vulnerability Advisory

ETN-VA-2021-1000: Multiple security issues in Intelligent Power Manager (IPM)

Date	Overall Risk	CVSS v3.0
04/12/2021	High	8.7

Overview

Eaton has been made aware of security vulnerabilities in its Intelligent Power Manager (IPM) software. Eaton's Intelligent Power Manager (IPM) software provides the tools needed to monitor and manage power devices in your physical or virtual environment. This innovative software solution ensures system uptime and data integrity by allowing you to remotely monitor, manage and control UPSs and other devices on your network. IPM provides a solution that is easy to use and maintains business continuity.

Vulnerability Details

CVE-2021-23276

CVSS v3 Base Score – 7.1:AV:A/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Eaton Intelligent Power Manager (IPM) prior to 1.69 is vulnerable to authenticated SQL injection. A malicious user can send a specially crafted packet to exploit the vulnerability. Successful exploitation of this vulnerability can allow attackers to add users in the data base.

CVE-2021-23277

CVSS v3 Base Score - 8.3: AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

CWE-95: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')

Eaton Intelligent Power Manager (IPM) prior to 1.69 is vulnerable to unauthenticated eval injection vulnerability. The software does not neutralize code syntax from users before using in the dynamic evaluation call in loadUserFile function under scripts/libs/utils.js. Successful exploitation can allow attackers to control the input to the function and execute attacker-controlled commands.

CVE-2021-23278

CVSS v3 Base Score – 8.7: AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:H

CWE-20: Improper Input Validation

Eaton Intelligent Power Manager (IPM) prior to 1.69 is vulnerable to authenticated arbitrary file delete vulnerability induced due to improper input validation at server/maps_srv.js with action removeBackground and server/node_upgrade_srv.js with action removeFirmware. An attacker can send specially crafted packets to delete the files on the system where IPM software is installed.

Eaton Vulnerability Advisory

CVE-2021-23279

CVSS v3 Base Score – 8.0: AV:A/AC:H/PR:N/UI:N/S:C/C:N/I:H/A:H

CWE-20: Improper Input Validation

Eaton Intelligent Power Manager (IPM) prior to 1.69 is vulnerable to unauthenticated arbitrary file delete vulnerability induced due to improper input validation in meta_driver_srv.js class with saveDriverData action using invalidated driverID. An attacker can send specially crafted packets to delete the files on the system where IPM software is installed.

CVE-2021-23280

CVSS v3 Base Score - 8.0: AV:A/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

CWE-434: Unrestricted Upload of File with Dangerous Type

Eaton Intelligent Power Manager (IPM) prior to 1.69 is vulnerable to authenticated arbitrary file upload vulnerability. IPM's maps_srv.js allows an attacker to upload a malicious NodeJS file using uploadBackgroud action. An attacker can upload a malicious code or execute any command using a specially crafted packet to exploit the vulnerability.

CVE-2021-23281

CVSS v3 Base Score - 8.3: AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

CWE-94: Improper Control of Generation of Code ('Code Injection')

Eaton Intelligent Power Manager (IPM) prior to 1.69 is vulnerable to unauthenticated remote code execution vulnerability. IPM software does not sanitize the date provided via coverterCheckList action in meta_driver_srv.js class. Attackers can send a specially crafted packet to make IPM connect to rouge SNMP server and execute attacker-controlled code.

Affected Product(s) and Version(s)

Here is the list of affected products –

- Eaton Intelligent Power Manager (IPM) – all versions prior to 1.69
- Eaton Intelligent Power Manager Virtual Appliance (IPM VA) – all versions prior to 1.69
- Eaton Intelligent Power Protector (IPP) – all versions prior to 1.68

Eaton Vulnerability Advisory

Remediation & Mitigation

Remediation

Eaton has patched these security issues and new versions of the affected software are released. The latest versions can be downloaded from below location: -

Eaton IPM v1.69 – Download | IPM | Eaton

Eaton IPP v1.68 – Download software | Power management | Eaton

Mitigation

To prevent the exploitation of the issues and safeguard the software from malicious entities, Eaton recommends blocking ports 4679 & 4680 at the enterprise network or home network where Intelligent Power Manager (IPM) software is installed and used.

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 researcher(s) for their coordinated support on the security vulnerabilities: -

- CVE-2021-23276 – Amir Preminger from Claroty research
- CVE-2021-23277 – Amir Preminger from Claroty research
- CVE-2021-23278 – Amir Preminger from Claroty research
- CVE-2021-23279 – Amir Preminger from Claroty research
- CVE-2021-23280 – Amir Preminger from Claroty research
- CVE-2021-23281 – Amir Preminger from Claroty research

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:

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.

Eaton Vulnerability Advisory

Revision Control:

Date	Version	Notes
04/12/2021	v1.0	Initial advisory

Office:

Eaton, 1000 Eaton Boulevard

Cleveland, OH 44122, United States

Eaton.com