Eaton Vulnerability Advisory

ETN-VA-2020-1004: Multiple Security Vulnerabilities v1.1

Publish Date	Affected Eaton Product(s) & Version(s)	CVE ID(s)	Severity
5/4/2020 Updated 5/7/2020	Intelligent Power Manager (IPM) v 1.67 & prior	CVE-2020-6651 CVE-2020-6652	High

Overview

Eaton has been made aware of security vulnerabilities in versions 1.67 or prior of its Intelligent Power Manager (IPM) which is used to monitor, manager & control devices on a remote network.

Vulnerability Details

CVE-2020-6651

CVSS v3 Base Score - 8.8: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CWE-20: Improper Input Validation

Eaton Intelligent Power Manager (IPM) v 1.67 & prior may not validate the import configuration file names properly. Successful exploitation of this vulnerability could allow an attacker to perform command injection or code execution via specially crafted file names while uploading the config file in the application. There are currently no reports of these vulnerabilities being exploited in the wild.

CVE-2020-6652

CVSS v3 Base Score – 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CWE-266: Incorrect Privilege Assignment

Eaton's Intelligent Power Manager (IPM) v1.67 & prior may allow non-administrator users to upload the system configuration files by sending specially crafted requests. Successful exploitation of this vulnerability can allow non-administrator users to manipulate the system configurations by uploading configurations with incorrect parameters.

Remediation & Mitigation

Remediation

Eaton has patched these security issues and a newer version 1.68 of the software is released. The latest version can be downloaded from below locations: -

Product Website - http://powerquality.eaton.fr/Support/Software-Drivers/Downloads/FR-Intelligent-Power-Software.asp

Eaton.com site – https://www.eaton.com/us/en-us/catalog/backup-power-ups-surge-it-power-distribution/eaton-intelligent-power-manager/download-eaton-intelligent-power-manager-ipm.html

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.

Product Description

Eaton's Intelligent Power Manager (IPM) software provides the tools needed to monitor and manage power equipment in a physical or virtual environment keeping IT devices up and running during a power or environmental event. This innovative software solution ensures system uptime and data integrity by allowing users to remotely monitor, manage and control devices on their networks.

General Security Best Practices

- Restrict exposure to external network for all control system devices and/or systems and ensure that they are not directly accessible from open internet.
- Deploy control system networks and remote devices behind barrier devices(e.g. firewall, data diode), and isolate them from the business network.
- Remote access to control system network shall be made available only on need to use basis. Remote access shall 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, DCP, etc.) on the devices.
- Create security zones for devices with common security requirements using barrier devices(e.g. firewall, data diode).
- Change default passwords following initial startup. Use complex secure passwords.
- Perform regular security assessments and risk analysis of your control systems.

For more details on Security best practices please follow below whitepapers –

- 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-2020-6651 – Sivathmican Sivakumaran of Trend Micro Zero Day Initiative
- CVE-2020-6652 – Sivathmican Sivakumaran of Trend Micro Zero Day Initiative

Additional Support and Information

For additional information or 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 you can contact us at CybersecurityCOE@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.

Powering Business Worldwide

Eaton Vulnerability Advisory

Revision Control:

Date	Version	Notes
5/4/2020	v1.0	Original release of the advisory.
5/7/2020	V1.1	Updated the notification ID and CVE description

Office:

Eaton, 1000 Eaton Boulevard

Cleveland, OH 44122, United States

Eaton.com