Eaton Vulnerability Advisory

ETN-VA-2021-1002b: Security issues in Eaton Intelligent Power Protector (IPP)

Date	Overall Risk	CVSS v3.1
02/08/2022	Medium	5.6

Overview

Eaton has been made aware of security vulnerabilities in Intelligent Power Protector (IPP) software.

Eaton's Intelligent Power Protector (IPP) software provides graceful, automatic shutdown of network devices during a prolonged power disruption, preventing data loss and saving work-in-progress. As part of Eaton's power network management system, IPP works alongside Eaton Intelligent Power Manager to deliver comprehensive power management and protection.

Vulnerability Details

CVE-2021-23288

Stored Cross Site Scripting:

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

CWE-79: Improper Neutralization of Input ('Cross-site Scripting')

Eaton Intelligent Power Protector (IPP) prior to version 1.69 is vulnerable to stored Cross site scripting attack. The vulnerability exists due to insufficient validation of input from certain resources by the IPP software. 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 Protector (IPP) – all versions prior to 1.69 release 166

Eaton Vulnerability Advisory

Remediation & Mitigation

Remediation

Eaton has patched the security issue and new version of the affected software has been released. The latest version can be downloaded from below location: -

Eaton IPP v1.69 – Download software | Power management | Eaton

Mitigation

Eaton recommends the users to follow the Security best practices and configure the logical access mechanisms provided in IPP to safeguard the application from unauthorized access. Use the available access control mechanisms in IPP properly to ensure that access to the system where IPP application is installed and to the application is restricted to legitimate users only. Ensure that the users are restricted to only the privilege levels necessary to complete their job roles/functions.

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)

Eaton Vulnerability Advisory

- Cybersecurity Best Practices Checklist Reminder (WP910003EN)

Acknowledgement

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

- CVE-2021-23288 – Andreas Finstad and Arthur Donkers

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
02/08/2022	v1.0	Initial Public advisory

Office:

Eaton, 1000 Eaton Boulevard

Cleveland, OH 44122, United States

Eaton.com