# Eaton Vulnerability Advisory

## ETN-VA-2022-1007: Update on Foreseer EPMS Vulnerabilities

| Publish Date | Affected Eaton Product(s) & Version(s) | CVE ID(s) | Severity |
|---|---|---|---|
| 10/12/2022 | Foreseer EPMS versions 4.x, 5.x, 6.x and 7.0 to 7.5 | CVE-2022-33859 | High |

## Overview

A security vulnerability was discovered in the Eaton Foreseer EPMS software. Foreseer EPMS connects an operation's vast array of devices to assist in the reduction of energy consumption and avoid unplanned downtime caused by the failures of critical systems. A threat actor may upload arbitrary files using the file upload feature.

This vulnerability is present in versions 4.x, 5.x, 6.x & 7.0 to 7.5. A new version (v7.6) containing the remediation has been made available by Eaton and a mitigation has been provided for the affected versions that are currently supported.

Customers are advised to update the software to the latest version (v7.6).

Foreseer EPMS versions 4.x, 5.x, 6.x are no longer supported by Eaton. Please refer to the End-of-Support notification.

## Vulnerability Details

**CVE-2022-33859**

CVSS v3 Base Score – 8.1 CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:L/I:H/A:H

CWE-434: Unrestricted file upload

A threat actor may upload arbitrary files using the file upload feature and execute a remote code.

## Remediation & Mitigation

### Remediation

Eaton has patched these security issues and an updated version of the Foreseer software has been released. For updating to the latest version (v7.6), please contact your local Eaton support executive.

### Mitigation Instructions

The mitigation is applicable to Foreseer EPMS v7.5 & prior only. The vulnerability may be mitigated by disabling the file upload feature. A Foreseer user with administrative access to the Foreseer server is required to perform the task. A server restart will also be required. This change will not affect the general use of the software.

# Eaton Vulnerability Advisory

Customers should follow the steps in the file below to disable the feature.

Foreseer- Steps to Disable File Upload.p

Customers should also use only Eaton Signed software executables for updates (right Click on executable properties and check for Eaton signature in the digital signatures tab).

## General Security Best Practices

- Restrict exposure to external network for all control system devices 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 information on Security best practices refer to the following:

- 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-2022-33859 – Michael

# Eaton Vulnerability Advisory

## 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; 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. YOU ARE SOLELY RESPONSIBLE FOR REVIEWING THE USER MANUAL FOR YOUR DEVICES AND GAINING KNOWLEDGE ON CYBERSECURITY MEASURES. YOU SHOULD TAKE NECESSARY STEPS TO ENSURE THAT YOUR DEVICE OR SOFTWARE IS PROTECTED, INCLUDING CONTACTING AN EATON PROFESSIONAL. 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, 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 85,000 employees and sells products to customers in more than 175 countries.

## Revision Control:

| Date | Version | Notes |
|---|---|---|
| 7/19/2022 | v1.0 | Original release of the advisory. |
| 10/12/2022 | v1.1 | Update on the public advisory. |

# Eaton Vulnerability Advisory

## Office:

Eaton, 1000 Eaton Boulevard

Cleveland, OH 44122, United States

Eaton.com