

Eaton Vulnerability Advisory

ETN-VA-2024-1009: Multiple security issues in Eaton Foreseer Reporting Software (FRS)

Date	Overall Risk	CVSS v3.0
02/26/2025	Medium	6.7

Overview

Eaton has released a new version of the Foreseer Reporting Software (FRS). The customers are requested to migrate to the secure version by updating their software. This patch fixes multiple security vulnerabilities with medium severity.

Vulnerability Details

CVE-2025-22491:

CVSS v3.1 Base Score – 6.7 [CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H](#)

CWE-20: Improper Input Validation

User input was not sanitized on Reporting Hierarchy Management page of FRS application which could lead into execution of arbitrary JavaScript in a browser context for all the interacting users.

CVE-2025-22492:

CVSS v3.1 Base Score – 6.3 [CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:L](#)

CWE-256: Plaintext Storage of a Password

Connection string visible to users with access to FRSCore database on FRS VM, this string can be used for gaining administrative access to the 4crXref database.

CVE-2025-22493:

CVSS v3.1 Base Score – 5.6 [CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:H/A:L](#)

CWE-614: Sensitive Cookie in HTTPS Session Without 'Secure' Attribute

CWE-1275: Sensitive Cookie with Improper SameSite Attribute

Secure flag not set and SameSite was set to Lax. Absence of this secure flag could lead into the session cookie being transmitted over unencrypted HTTP connections.

Affected Product(s) and Version(s)

Eaton Foreseer Reporting Software (FRS) – All versions up to 1.5.100 (excluding)

Eaton Vulnerability Advisory

Remediation & Mitigation

Remediation

Eaton has remediated these issues in the latest release of FRS version 1.5.100. Please contact your local Eaton support executive for the patched version.

Eaton highly recommends that customers and or end-users implement these patches as soon as possible.

Mitigation

Eaton recommends implementing the below mitigation measures only in the case where the users are unable to apply the above patches.

- Restrict remote and local access to the host system to authorized personnel only.
- Refrain from sharing credentials.
- Ensure control system PCs, networks and remote devices are placed behind securely configured firewalls.
- Restrict physical access to the FRS to authorized personnel only.

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

Eaton Vulnerability Advisory

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](#))

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. YOU ARE SOLELY RESPONSIBLE FOR REVIEWING THE USER MANUAL FOR YOUR DEVICES AND GAINING KNOWLEDGE ON CYBERSECURITY MEASURES. YOU SHOULD TAKE THE 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 using power management technologies and services. Eaton has approximately 85,000 employees and sells products to customers in more than 175 countries.

Eaton Vulnerability Advisory

Revision Control:

Date	Version	Notes
02/26/2025	v1.0	Initial Notification

Office:

Eaton, 1000 Eaton Boulevard
Cleveland, OH 44122, United States
Eaton.com