Eaton Vulnerability Advisory

ETN-VA-2024-1008: Multiple vulnerabilities identified in Foreseer

Date	Overall Risk	CVSS v3.1
09/13/2024	Medium	6.7

Overview

Eaton has released a new version of the Foreseer software. Customers are strongly advised to update their software to the new version of the software in order to remediate the discovered vulnerabilities. This patch fixes multiple security vulnerabilities with medium severity.

Vulnerability Details

CVE-2024-31414:

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-79: Improper Neutralization of Input During Web Page Generation
Improper server-side sanitization of input on the Foreseer application could lead to injection and execution of malicious scripts.

CVE-2024-31415:

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-522: Insufficiently Protected Credentials
The keys used for encrypting server configurations was insecurely stored on the host machine which could be abused to possibly change or remove the server configuration.

CVE-2024-31416:

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-1284: Improper Validation of Specified Quantity in Input
The input fields in the Foreseer software do not check the length and bounds of the entered value which may result in excessive memory consumption or integer overflow.

Affected Product(s) and Version(s)

Eaton Foreseer – versions up to 7.8.600 (excluding)

Remediation & Mitigation

Remediation

Eaton has remediated these issues in the latest release of Foreseer version 7.8.600. Please contact your local Eaton support executive for the patched version.

Eaton Vulnerability Advisory

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 Foreseer 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 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-2024-31415 - Joseph Yim (Packet Labs)

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 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
09/13/2024	v1.0	Initial notification

Office:

Eaton, 1000 Eaton Boulevard

Cleveland, OH 44122, United States

Eaton.com