

Eaton Vulnerability Advisory

ETN-VA-2025-1022: Vulnerability reported in Eaton xComfort ECI

Date	Overall Risk	CVSS v3.0
12/22/2025	High	8.8

Overview

Eaton has been notified about a security vulnerability affecting Eaton's xComfort ECI. The router is used to provide ethernet communication interface to xComfort RF devices. As cybersecurity standards continue to evolve and to meet our requirements today, we have decided to discontinue the product. Upon retirement or end of support, there will be no new security updates, non-security updates, or paid assisted support options, or online technical content updates.

Vulnerability Details

CVE-2025-59886

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

Due to improper input validation at one of the endpoints of web interface, an attacker with network access to the device could execute privileged user commands.

Affected Product(s) and Version(s)

Eaton xComfort ECI – All versions

Remediation & Mitigation

Remediation

Eaton has decided to end-of-life xComfort ECI effective November 30, 2025. (End-of-life notification - [Link](#))

Eaton recommends implementing the mitigation measures below.

Mitigation

Eaton recommends implementing the mitigation measures below in case if the above remediation is not feasible -

- Ensure that the router is configured to a secure network. Do not leave the router unconfigured.
- Change the default credentials of the router to a complex or a unique alpha-numeric password with special characters.
- Only permit trusted devices to connect to the router.
- Ensure that the software of the router is updated to the latest version.
- Ensure a firewall functionality is configured connecting to the router to prevent malicious traffic.

Eaton Vulnerability Advisory

- When remote access is required to the devices, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPNs are only as secure as the connected devices.

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](#))
- Cybersecurity Best Practices Checklist Reminder ([WP910003EN](#))

Acknowledgement

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

- CVE-2025-59886 – Mihkal Dunfjeld

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.

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
12/22/2025	v1.0	Initial advisory

Office:

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