

Eaton Vulnerability Advisory

ETN-VA-2025-1002: Multiple vulnerabilities detected in Eaton G4 PDU

Date	Overall Risk	CVSS v3.0
08/06/2025	Medium	5.7

Overview

Eaton has released a new firmware version of Eaton Rack PDU G4. The customers are requested to migrate to the secure version by updating their software. This patch fixes multiple security vulnerabilities with medium severity in Eaton G4 PDU.

Vulnerability Details

[CVE-2025-48393](#)

CVSS v3.1 Base Score – 5.7 [CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:L/A:L](#)

The server identity check mechanism for firmware upgrade performed via command shell is insecurely implemented potentially allowing an attacker to perform a Man-in-the-middle attack.

[CVE-2025-48394](#)

CVSS v3.1 Base Score – 4.7 [CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L](#)

An attacker with authenticated and privileged access could modify the contents of a non-sensitive file by traversing the path in the limited shell of the CLI.

Affected Product(s) and Version(s)

Eaton Rack PDU G4 - All versions up to 3.5.0

Remediation & Mitigation

Remediation

Eaton has remediated these issues in the latest firmware release of Eaton Rack PDU G4 version 3.5.0. Please contact your local Eaton support executive or refer to the following link for the patched version – [link](#). Eaton highly recommends that customers and/or end-users implement these patches as soon as possible.

Mitigation

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

- Restrict network access to the affected products by leveraging the IP whitelisting functionality.

Eaton Vulnerability Advisory

- Ensure control system networks and remote devices are placed behind securely configured firewalls.
- Restrict the SSH access to authorized users only.

Additionally, customers are requested to follow the cybersecurity best practices to further protect their devices, as outlined below.

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 researcher below for their coordinated support on the security vulnerabilities: -

- CVE-2025-48393 – Harry Sintonen
- CVE-2025-48394 – Harry Sintonen

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
08/06/2025	v1.0	Initial advisory

Office:

Eaton, 1000 Eaton Boulevard

Cleveland, OH 44122, United States

Eaton.com