Product support

Security Advisories

SUMMARY

CVE-2026-3867, CVE-2026-3868: Improper Ownership Management and Improper Handling of Length Parameter Inconsistency Vulnerabilities in Secure Router

Security Advisory ID: MPSA-261521
Version: V1.0
Release Date: Apr 27, 2026
Reference:

- CVE-2026-3867 (CNA: Moxa)
- CVE-2026-3868 (CNA: Moxa)

This security advisory addresses two vulnerabilities identified in Secure Router.

CVE-2026-3867

An improper ownership management vulnerability has been identified in Moxa's Secure Router. Because of improper ownership management, a low-privileged authenticated user may access a configuration file containing the hashed password of the administrative account. Successful exploitation of this vulnerability could allow an attacker to obtain sensitive information. Exploitation is only possible under a specific condition — when the configuration file has been exported. This vulnerability does not impact the integrity or availability of the affected product and has no integrity, or availability impact to the subsequent system.

CVE-2026-3868

An improper handling of the length parameter inconsiste[illegible]s in Moxa's Secure Router. Because of improper validation of length parameters in the HTTPS

management interface, an unauthenticated remote attacker could send specially crafted requests that trigger a buffer overflow condition, causing the web service to become unresponsive. Successful exploitation may result in a denial-of-service condition requiring a device reboot to restore normal operation. While successful exploitation can severely impact the availability of the affected device, no impact to the confidentiality or integrity of the affected product has been identified. Additionally, no confidentiality, integrity, or availability impact to the subsequent system has been identified.

Given the high severity of CVE-2026-3868, users should apply the solutions immediately to reduce security risks.

The Identified Vulnerability Type and Potential Impact

CVE ID	VULNERABILITY TYPE	IMPACT
CVE-2026-3867	CWE-282: Improper Ownership Management	CAPEC-12 Abuse
CVE-2026-3868	CWE-130: Improper Handling of Length Parameter Inconsistency	CAPEC-47 via Parame

Vulnerability Scoring Details

CVE ID	BASE SCORE	VECTOR
CVE-2026-3867	CVSS 4.0: 6.0	AV:N/AC:L/AT:P/PR:L/UI:N/ VC:H/VI:N/VA:N/SC:N/SI:N/SA:N
CVE-2026-3868	CVSS 4.0: 8.7	AV:N/AC:L/AT:N/PR:N/UI:N/ VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

AFFECTED PRODUCTS AND SOLUTIONS

Solutions

Moxa has developed appropriate solutions to address these vulnerabilities. The solutions for the affected products are listed in the following table:

PRODUCT SERIES	AFFECTED VERSIONS	SOLUTIONS
TN-4900 Series	Firmware v3.22 and earlier	Firmware v3.24 or later
EDR Series • EDR-8010 Series • EDR-G9010 Series	Firmware • v3.23 and earlier • v3.23.1 and earlier	Firmware • v3.24 or later • v3.24 or later
OnCell Series • OnCell G4302-LTE4 Series • OnCell G4308-LTE4 Series	Firmware • v3.23.0 and earlier • v3.23.0 and earlier	Please contact Moxa Tech the security patch (v3.24.1
EDF-G1002-BP Series	Firmware v3.23 and earlier	Firmware v3.24 or later

Mitigations

For users who may not be able to perform a firmware update, we provide the following recommended mitigation measures as an alternative to mitigate the risk associated with the vulnerability.

- Refer to the **General Security Recommendations** section to further strengthen your security context.

General Security Recommendations

Revision History:

VERSION	DESCRIPTION	RELEASE DATE
1.0	First release	April 27, 2026

Relevant Products

EDF-G1002-BP Series · EDR-8010 Series · EDR-G9010 Series · OnCell G4302-LTE4 Series · OnCell G4308-LTE4 Series · TN-4900 Series ·

Related Advisories

- Missing Authentication and OS Command Injection Vulnerabilities in Cellular Routers, Secure Routers, and Network Security Appliances
- CVE-2025-0415: Command Injection Leading to Denial-of-Service in Secure Routers, Cellular Routers, and Network Security Appliances
- CVE-2025-0676: Command Injection Leading to Privilege Escalation in Secure Routers, Cellular Routers, Network Security Appliances
- CVE-2025-6892, CVE-2025-6893, CVE-2025-6894, CVE-2025-6949, CVE-2025-6950: Multiple Vulnerabilities in Network Security Appliances and Routers
- Privilege Escalation and OS Command Injection Vulnerabilities in Cellular Routers, Secure Routers, and Network Security Appliances