OpenSSL Vulnerabilities in NRSW

Date: 2026-04-02
Version: 1.0

Summary

CVE-2025-69419 and CVE-2025-15467 require the system to parse malicious or otherwise untrusted certificate related data. In normal deployments, only trusted certificates or trusted encrypted messages are processed. The practical risk becomes meaningful only if an administrator manually installs such malicious files, or if a remote system that supplies certificate-based data is compromised.

The following vulnerability affects one or more versions of the products listed in the next section:

ID	Title / Description	Severity
CVE-2025-15457	Stack buffer overflow in CMS AuthEnvelopedData parsing	CVSS v3.1: 8.8
CVE-2025-69419	Out of bounds write in PKCS12_get_friendlyname() UTF-8 conversion	CVSS v3.1: 7.4

Affected Products

Brand	Product Line	Affected Version(s)
NetModule	NetModule Router Software	5.0.0.101 and lower

Mitigation

We recommend upgrading to version 5.0.0.102 or later.

For Help or Feedback

To view all Belden Security Advisories or to report suspected security vulnerabilities, go to https://www.belden.com/security.
For technical support and other requests, please visit https://www.belden.com/support/technical-product-support-main.

Related Links

- CVE-2025-15467
- CVE-2025-69419

Disclaimer

Revisions

V1.0 (2026-04-02) Security Advisory published.