Unsigned Firmware Update Tampering

Date: 2026-06-19
Version: 1.0

Summary

The Rail Data Diode (RDD) does not enforce cryptographic signature verification of firmware update packages and may be exposed to a firmware tampering risk during the update process.

The firmware packages rely on checksums or hashes that can be recomputed after modification, rather than on a trusted digital signature. As a result, an authenticated attacker with privileged access to the device management interface could modify a legitimate firmware update package, add unauthorized functionality or arbitrary code, and install the tampered package without the device detecting the modification.

ID	Title / Description	Severity
CWE-494	Download of Code Without Integrity Check	CVSS v4.0: 8.6

Affected Products

Brand	Product Line	Affected Version(s)
Hirschmann	Rail Data Diode (RDD)	All

Mitigation

Belden recommends the following measures to reduce risk on affected products:

- Download firmware only from official Belden sources and verify integrity using trusted channels.
- Verify firmware checksums before installation using values obtained from a trusted Belden channel.
- Restrict access to management interfaces using network segmentation, firewalls, and ACLs.

These measures reduce exposure significantly but do not eliminate the underlying risk.

Acknowledgments

Belden would like to thank Nozomi Networks Labs, and in particular Luca Borzacchiello, for reporting this issue and for coordinating disclosure with Belden.

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

- [1] CWE - CWE-494: Download of Code Without Integrity Check (4.20)

Disclaimer

Revisions

V1.0 2026-06-19	Security Advisory published.