

Multiple OpenSSL vulnerabilities in various products

Date: <2023-11-27> | Updated: <2024-03-14>

Version: 1.0

Summary

The following vulnerabilities affect one or more versions of the products listed in the next section:

ID	Title / Description	Severity
CVE-2023-0286	There is a type confusion vulnerability relating to X.400 address processing inside an X.509 GeneralName.	CVSS v3.1: 7.4
CVE-2022-4304	A timing based side channel exists in the OpenSSL RSA Decryption implementation which could be sufficient to recover a plaintext across a network in a Bleichenbacher style attack.	CVSS v3.1: 5.9
CVE-2023-0215	The public API function BIO_new_NDEF is a helper function used for streaming ASN.1 data via a BIO.	CVSS v3.1: 7.5
CVE-2022-4450	The function PEM_read_bio_ex() reads a PEM file from a BIO and parses and decodes the "name" (e.g. "CERTIFICATE"), any header data and the payload data.	CVSS v3.1: 7.5

Affected Products

Brand	Product Line / Platform	Product	Version
Hirschmann	HiSecOS	EAGLE	04.5.00 or lower
Hirschmann	Classic Firewall	EAGLE One	05.4.03 or lower
Hirschmann	HiOS	RSP, RSPE, MSP, GRS, OS, DRAGON, BRS	09.2.01 or lower
Hirschmann	HiOS	RSP-2S, RSPL, RED, RSPS, GRS1020/30	07.1.06 or lower
Hirschmann	Classic Switch	RS, RSR, RSB, MACH100, MACH1000, MACH4000, MS, OCTOPUS	09.1.09 or lower
Hirschmann	HiLCOS	BAT	10.34-RU4 or lower
Hirschmann	OWL	OWL	6.3.7 or lower

Solution

Updates are available, which address the vulnerability. Customers are advised to update their product.

Brand	Product Line / Platform	Product	Version
Hirschmann	HiSecOS	EAGLE	04.6.02 or higher
Hirschmann	Classic Firewall	EAGLE One	05.4.04 or higher
Hirschmann	HiOS	RSP, RSPE, MSP40, GRS, OS, BRS, BXS	09.4.00 or higher
Hirschmann	HiOS	RSP-2S, RSPL, RED, RSPS, GRS1020/30	07.1.08 or higher
Hirschmann	Classic Switch	RS, RSR, RSB, MACH100, MACH1000, MACH4000, MS, OCTOPUS	09.1.10 or higher
Hirschmann	HiLCOS	BAT	10.34-RU5 or higher
Hirschmann	OWL	OWL	6.3.10 or higher

For Help or Feedback

To view all Belden Security Bulletins or to report suspected security vulnerabilities, go to <https://www.belden.com/security>.

For technical support and other requests, please visit <https://hirschmann-support.belden.com> and <https://garrettcom-support.belden.com>.

Related Links

- <https://nvd.nist.gov/vuln/detail/CVE-2023-0286>
- <https://nvd.nist.gov/vuln/detail/CVE-2022-4304>
- <https://nvd.nist.gov/vuln/detail/CVE-2023-0215>
- <https://nvd.nist.gov/vuln/detail/CVE-2022-4450>
- <https://nvd.nist.gov/vuln/detail/CVE-2022-2097>

Disclaimer

THE SECURITY BULLETIN, AND INFORMATION CONTAINED HEREIN, ARE PROVIDED ON AN "AS IS" BASIS AND DO NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE BULLETIN, AND INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED FROM THE BULLETIN, IS AT YOUR OWN RISK. INFORMATION IN THIS BULLETIN AND ANY RELATED COMMUNICATIONS IS BASED ON OUR KNOWLEDGE AT THE TIME OF PUBLICATION AND IS SUBJECT TO CHANGE WITHOUT NOTICE. BELDEN RESERVES THE RIGHT TO CHANGE OR UPDATE BULLETINS AT ANY TIME.

Revisions

V1.0 (<2023-11-27>): Bulletin created.