Multiple libexpat vulnerabilities in HiOS, Classic, HiSecOS, Wireless BAT-C2, Lite Managed, Edge

Date: 2023-04-25
Version: 1.0

Summary

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

ID	Title / Description	Severity
CVE-2022-40674	libexpat before 2.4.9 has a use-after-free in the doContent function in xmlparse.c.	CVSS v3.1: 9.8[1]
CVE-2022-43680	In libexpat through 2.4.9, there is a use-after free caused by overeager destruction of a shared DTD in XML_ExternalEntityParserCreate in out-of-memory situations.	CVSS v3.1: 7.5[2]

Affected Products

Brand	Product Line / Platform	Product	Version
Hirschmann	HiOS	BRS, RSP, RSPE, RSPS, RSPL, MSP, EES, EESX, GRS, OS, RED	09.1.XX or lower 09.0.05 or lower 07.1.07 or lower
	Classic	RS, RSR, RSB, MACH100, MACH1000, MACH4000, MS, OCTOPUS	09.1.07 or lower
	HiSecOS	EAGLE	04.3.XX or lower
	Wireless BAT-C2	BAT-C2	9.14.1.0R2 or lower
	Lite Managed	GECKO	2.3.2 or lower
	Edge	OpEdge-8D	01.0.00

Solution

Updates are available, which address the vulnerability. Customers are advised to update their product. In case no update is available yet, please refer to the mitigation section.

Brand	Product Line / Platform	Product	Version
Hirschmann	HiOS	BRS, RSP, RSPE, RSPS, RSPL, MSP, EES, EESX, GRS, OS, RED	09.2.00 or higher Upcoming releases: 09.0.06 or higher 07.1.08 or higher
	Classic	RS, RSR, RSB, MACH100, MACH1000, MACH4000, MS, OCTOPUS	09.1.08 or higher
	HiSecOS	EAGLE	04.4.00 or higher
	Wireless BAT-C2	BAT-C2	9.14.1.0R3 or higher
	Lite Managed	GECKO	2.3.3 or higher
	Edge	OpEdge-8D	Upcoming release: 01.0.01 or higher

Mitigation

Customers are advised to follow security best practices and restrict usage to required functionalities. Following product line specific mitigation may additionally be applied:

HiOS/HiSecOS: Disable HTTP/HTTPS server or restrict access to HTTP/HTTPS to trusted IP addresses.
Edge: Disable HTTP/HTTPS server or restrict access to HTTP/HTTPS to trusted IP addresses using the 'Allowed IP List' under the 'Systems' tab.

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.

Related Links

- [1] https://nvd.nist.gov/vuln/detail/CVE-2022-40674
- [2] https://nvd.nist.gov/vuln/detail/CVE-2022-43680

Disclaimer

Revisions

V1.0 (2023-04-25):	Bulletin created.