Multiple BusyBox vulnerabilities in BAT-C2 and OWL

Date: 2024-05-13
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-2021-28831[1]	decompress_gunzip.c in BusyBox through 1.32.1 mishandles the error bit on the huft_build result pointer, with a resultant invalid free or segmentation fault, via malformed gzip data.	CVSS v3.1: 7.5
CVE-2022-28391[2]	BusyBox through 1.35.0 allows remote attackers to execute arbitrary code if netstat is used to print a DNS PTR record's value to a VT compatible terminal. Alternatively, the attacker could choose to change the terminal's colors.	CVSS v3.1: 8.8
CVE-2022-30065[3]	A use-after-free in Busybox 1.35-x's awk applet leads to denial of service and possibly code execution when processing a crafted awk pattern in the copyvar function.	CVSS v3.1: 7.8

Affected Products

CVE-2021-28831

Brand	Product Line / Platform	Product	Version
Hirschmann	BAT-C2	BAT-C2	08.08.01.01R08 or lower

CVE-2022-28391

Brand	Product Line / Platform	Product	Version
Hirschmann	OWL	OWL 3G, OWL LTE, OWL LTE M12	6.2.9 or lower

Solution

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

Brand	Product Line / Platform	Product	Version
Hirschmann	BAT-C2	BAT-C2	9.13.1.0R2 or higher
Hirschmann	OWL	OWL 3G, OWL LTE, OWL LTE M12	6.3.7 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.

Related Links

- [1] https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28831
- [2] https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-28391
- [3] https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30065

Disclaimer

Revisions

V1.0 (2024-05-13):	Bulletin released.