

Multiple vulnerabilities in Provize Basic Frontend

Date: 2022-05-03

Version: 1.0

Summary

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

ID	Title / Description	Severity
CVE-2021-23406	This affects the package pac-resolver before 5.0.0. This can occur when used with untrusted input, due to unsafe PAC file handling	CVSS v3.1: 9.8
CVE-2021-37712	The npm package "tar" (aka node-tar) before versions 4.4.18, 5.0.10, and 6.1.9 has an arbitrary file creation/overwrite and arbitrary code execution vulnerability	CVSS v3.1: 8.6
CVE-2021-37701	The npm package "tar" (aka node-tar) before versions 4.4.16, 5.0.8, and 6.1.7 has an arbitrary file creation/overwrite and arbitrary code execution vulnerability	CVSS v3.1: 8.6
CVE-2021-37713	The npm package "tar" (aka node-tar) before versions 4.4.18, 5.0.10, and 6.1.9 has an arbitrary file creation/overwrite and arbitrary code execution vulnerability	CVSS v3.1: 8.6
CVE-2021-32803	The npm package "tar" (aka node-tar) before versions 6.1.2, 5.0.7, 4.4.15, and 3.2.3 has an arbitrary File Creation/Overwrite vulnerability via insufficient symlink protection	CVSS v3.1: 8.1
CVE-2021-32804	The npm package "tar" (aka node-tar) before versions 6.1.1, 5.0.6, 4.4.14, and 3.3.2 has a arbitrary File Creation/Overwrite vulnerability due to insufficient absolute path sanitization	CVSS v3.1: 8.1
CVE-2020-28469	This affects the package glob-parent before 5.1.2. The enclosure regex used to check for strings ending in enclosure containing path separator	CVSS v3.1: 7.5
CVE-2021-33623	The trim-newlines package before 3.0.1 and 4.x before 4.0.1 for Node.js has an issue related to regular expression denial-of-service (ReDoS) for the .end() method	CVSS v3.1: 7.5

Affected Products

Brand	Product Line / Platform	Product	Version
Belden	-	Provize Basic	01.1.01

Solution

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

Brand	Product Line / Platform	Product	Version
Belden	-	Provize Basic	01.1.02

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

- [1] <https://nvd.nist.gov/vuln/detail/CVE-2021-23406>
- [2] <https://nvd.nist.gov/vuln/detail/CVE-2021-37712>
- [3] <https://nvd.nist.gov/vuln/detail/CVE-2021-37701>
- [4] <https://nvd.nist.gov/vuln/detail/CVE-2021-37713>
- [5] <https://nvd.nist.gov/vuln/detail/CVE-2021-32803>
- [6] <https://nvd.nist.gov/vuln/detail/CVE-2021-32804>
- [7] <https://nvd.nist.gov/vuln/detail/CVE-2020-28469>
- [8] <https://nvd.nist.gov/vuln/detail/CVE-2021-33623>

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 (2022-05-03)

Bulletin published.