Belden Security Bulletin – Industrial IT
BSECV-2021-27

DNS request vulnerability in Firewall Products

Date: 2023-07-25
Version: 1.0

Summary

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

ID	Title / Description	Severity
CVE-2021-43523[1]	In uClibc and uClibc-ng before 1.0.39, incorrect handling of special characters in domain names returned by DNS servers via gethostbyname, getaddrinfo, gethostbyaddr, and getnameinfo can lead to output of wrong hostnames (leading to domain hijacking) or injection into applications (leading to remote code execution, XSS, applications crashes, etc.).	CVSSv3.1: 9.6

Affected Products

Brand	Product Line / Platform	Product	Version
Hirschmann	HiSecOS	EAGLE	04.2.01 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	04.3.00

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-2021-43523

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 (2023-07-25):	Bulletin created.