StrongSwan vulnerability in Eagle and OWL

Date: 2023-04-24
Version: 1.0

Summary

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

ID	Title / Description	Severity
CVE-2021-41991[1]	strongSwan: integer overflow when replacing certificates in cache	CVSS v3.1: 7.5

Affected Products

Brand	Product Line / Platform	Product	Version
Hirschmann	HiSecOS	EAGLE	04.4.xx or lower
Hirschmann	Cellular Router	OWL	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	HiSecOS	EAGLE	4.5.0 or higher
Hirschmann	Cellular Router	OWL	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://nvd.nist.gov/vuln/detail/CVE-2021-41991

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 (2023-03-16):   Bulletin created.