

strongSwan vulnerability in HiSecOS

Date: June 6, 2018

Version: 1.0

Summary

The following vulnerability affects the IPsec functionality in one or more versions of the products listed in the next section:

ID	Title / Description	Severity
CVE-2017-9023	Incorrect Handling of CHOICE types in ASN.1 parser and x509 plugin	CVSS v3.0: 7.5

Affected Products

Brand	Product Line / Platform	Product	Version
Hirschmann	HiSecOS	EAGLE	03.1.00 and lower

Solution

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

Brand	Product Line / Platform	Product	Version
Hirschmann	HiSecOS	EAGLE	03.1.00

For Help or Feedback

To view all Belden Security Advisories and 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>.

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 (June 6, 2018): Bulletin created.