

TinyXML vulnerability in Hirschmann HiLCOS products

Date: 2022-11-23

Version: 1.0

Summary

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

ID	Title / Description	Severity
CVE-2021-42260 ¹	TinyXML through 2.6.2 has an infinite loop in TiXmlParsingData::Stamp in tinyxmlparser.cpp via the TIXML_UTF_LEAD_0 case. It can be triggered by a crafted XML message and leads to a denial of service	CVSS v3.1: 7.5

Affected Products

Brand	Product Line / Platform	Product	Version
Hirschmann	HiLCOS	OpenBAT, WLC, BAT450, BAT867, BATOne, BAT-Controller Virtual	8.60 or higher

Solution

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

Brand	Product Line / Platform	Product	Version
Hirschmann	HiLCOS	OpenBAT, WLC, BAT450, BAT867, BATOne, BAT-Controller Virtual	10.34-RU3 10.12-RU10

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-2021-42260>

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 (2022-11-23): Bulletin created.