

Potential denial of service vulnerability in PROFINET Devices via DCE-RPC Packets

Date: 2021-10-21

Version: 1.0

References: CVE-2019-13946¹

Executive Summary

A vulnerability in the PROFINET stack implementation in Classic Firmware, HiOS, and HiLCOS could lead to a denial of service via an out of memory condition.

Details

The PROFINET stack implementation does not properly limit internal resource allocation when multiple legitimate diagnostic package requests are sent to the DCE-RPC interface, which can lead to a denial of service condition.

The CVSS score of the vulnerability is rated as 7.5 (High) ¹:

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Impact

An attacker could use the vulnerability to compromise the availability of the device.

Affected Products

Brand	Product Line / Platform	Product	Version
Hirschmann	Classic	RS, RSR, RSB, MACH100, MACH1000, MACH4000, MS, OCTOPUS	Since 03.0.00
Hirschmann	HiOS	RSP, RSPE, RSPS, OS2, RED, EES, MSP, OS3, GRS1040.	since 05.0.00
Hirschmann	HiLCOS	BAT54-Rail (only)	V8.52 or older

Solution

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

Brand	Product Line / Platform	Product	Version
Hirschmann	Classic	RS, RSR, RSB, MACH100, MACH1000, MACH4000, MS, OCTOPUS	Fixed in 09.1.04
Hirschmann	HiOS	RSP, RSPE, RSPS, OS2, RED, EES, MSP, OS3, GRS1040.	Fixed in 08.4.00
Hirschmann	HiLCOS	BAT54-Rail (only)	Fixed in V8.80

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-2019-13946>

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 (2021-10-21): Bulletin published.