

Hirschmann RSP, RSPE, and OS2 series HSR denial of service vulnerability

Date: 2021-01-28

Version: 1.0

References: CVE-2020-9307¹

Executive Summary

A crafted HSR frame can cause a denial of service on one of the ports in an HSR ring.

Details

A change in the HSR implementation of the RSP, RSPE, or OS2 devices in HiOS 07.0.04 introduced a vulnerability. It could allow an unauthenticated, adjacent attacker to cause a denial of service on one of the HSR ring ports of the device.

The CVSS v3.1 severity of this vulnerability is 6.5 (medium):

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

Impact

A successful attack on a device in an HSR ring causes one of the ports in the ring to no longer switch packets, effectively breaking the redundancy of the HSR ring. If the attacker can perform the same attack on a second device, the ring is broken into two parts, thus disrupting communication between devices in the different parts.

Affected Products

Brand	Product Line / Platform	Product	Version
Hirschmann	HiOS	RSP, RSPE, OS2	07.0.04 – 07.1.00 08.0.00 – 08.3.xx

Solution

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

Brand	Product Line / Platform	Product	Version
Hirschmann	HiOS	RSP, RSPE, OS2	07.1.01 or higher 08.4.00 or higher

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>.

Acknowledgments

Belden thanks the following for working with us to help protect customers:

- The French National Cybersecurity Agency (ANSSI)

Related Links

- [1] <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9307>

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 (2021-01-28): Bulletin published.