HiOS EtherNet/IP stack vulnerability

Date: 2020-09-09
Version: 1.0

Executive Summary

The HiOS industrial protocol EtherNet/IP stack is vulnerable to EtherNet/IP packets with incorrect length field.

Details

On a device with the industrial protocol EtherNet/IP enabled, sending UDP EtherNet/IP packets to the device with a length in the header that is larger than the actual packet length can cause a crash or hang of the EtherNet/IP stack within the switch device.

Impact

The switch device can be crashed or brought into an inoperable state if the industrial protocol EtherNet/IP is enabled on the device and an attacker sends corrupted UDP EtherNet/IP packet(s) to the IP address/EtherNet/IP UDP port of the device.

Affected Products

Brand	Product Line / Platform	Product	Version
Hirschmann	HiOS	RSP, RSPE, RSPS, MSP, EES, GRS1040, OS, RED, BRS	08.0.00 and lower (starting with 05.0.00, which introduced EtherNet/IP support)

Solution

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

Brand	Product Line / Platform	Product	Version
Hirschmann	HiOS	RSP (2A/3S), RSPE, MSP, GRS1040, OS, BRS	08.1.00 or higher
Hirschmann	HiOS	RSP (2S), RSPS, EES, RED	07.1.01 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.

Disclaimer

Revisions

V1.0 (2020-09-09):	Bulletin created.