HiOS TCP Initial Sequence Number Predictability

Date: June 6, 2016
Version: 1.0
References: CVE-2015-3963, ICSA-15-169-01

Executive Summary

HiOS products with versions lower than 05.0.00 generate predictable TCP initial sequence numbers. This may allow an attacker to predict the TCP initial sequence numbers from previous values and to spoof or disrupt TCP connections. Customers are advised to update to software version 05.0.00 or higher.

Details

For details please see the ICS-CERT advisory ICSA-15-169-01.

Impact

TCP connections to the management software of an affected HiOS product may be disrupted or spoofed by an attacker with network access to the device.

Affected Products

Brand	Product Line / Platform	Product	Version
Hirschmann	HiOS	RSP, RSPS, RSPL, RSPE, MSP, GRS, OS, RED, EES, EESX	< 05.0.00

Solution

It is recommended to update affected products to version 05.0.00 or higher [3].

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.eu.com.

Related Links

- [1] ICSA-15-169-01
  https://ics-cert.us-cert.gov/advisories/ICSA-15-169-01
- [2] CVE-2015-3963:
  https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-3963
- [3] HiOS 05.0 - Hirschmann Operating Software:
  https://e-catalog.beldensolutions.com/link/57078-24455-278205-377857-436230/en/conf/0

Disclaimer

Revisions

V1.0 (June 6, 2016): Security Bulletin created.