Multiple NTP vulnerabilities in HiSecOS

Date: 2023-07-25
Version: 1.0

Summary

The following vulnerabilities affect one or more versions of the products listed in the next section:

ID	Title / Description	Severity
CVE-2020-15025[1]	Allows remote attackers to cause a denial of service (memory consumption) by sending packets	CVSSv3.1: 4.9
CVE-2020-13817[2]	Allows remote attackers to cause a denial of service (daemon exit or system time change) by predicting transmit timestamps for use in spoofed packets.	CVSSv3.1: 7.4
CVE-2020-11868[3]	Allows an off-path attacker to block unauthenticated synchronization via a server mode packet with a spoofed source IP address	CVSSv3.1: 7.5
CVE-2018-8956[4]	Allow remote attackers to prevent a broadcast client from synchronizing its clock with a broadcast NTP server via spoofed mode 3 and mode 5 packets.	CVSSv3.1: 5.3

Affected Products

Brand	Product Line / Platform	Product	Version
Hirschmann	HiSecOS	EAGLE	3.5.0 to 4.2.02

Solution

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

Brand	Product Line / Platform	Product	Version
Hirschmann	HiSecOS	EAGLE	04.3.00

Mitigation: Configure only trusted NTP server(s) and ensure that an attacker cannot inject spoofed NTP packets in your network.

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-2020-15025
- [2] https://nvd.nist.gov/vuln/detail/CVE-2020-13817
- [3] https://nvd.nist.gov/vuln/detail/CVE-2020-11868
- [4] https://nvd.nist.gov/vuln/detail/CVE-2018-8956

Disclaimer

Revisions

V1.0 (2023-07-25):	Bulletin created.