Web interface vulnerability in HiLCOS.

Date: <2024-09-16> | Updated: <2024-10-16>
Version: 1.0

Summary

A vulnerability in HiLCOS web interface allows a remote attacker to trigger a Denial of Service attack (DoS), even without authentication.

ID	Severity
SSD Advisory Heap Overflow [1]	CVSS v3.1: 7.0 [2]

Details

The web interface (HTTPs) is enabled by default on all LAN interfaces on TCP port 443. Custom configurations could run it on other ports or on TCP port 80 as HTTP as well. Customers using the Public Spot functionality are advised to update immediately or turn off the Public Spot functionality until then.

A workaround is to turn off the web interface completely, or block it with a firewall in scenarios where a software upgrade is not immediately possible. Management products like Hirschmann LANConfig, the WLC and BAT Controller Virtual fall back to other methods like SSH automatically.

Affected Products

Brand	Product Line / Platform	Product	Version
Hirschmann	HiLCOS	BAT-R, BAT-F, BAT450-F, BAT867-R, BAT867-F, WLC, BAT Controller Virtual	HiLCOS 10.34.6313 (Release Update 7) and lower

Solution

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

Brand	Product Line / Platform	Product	Version
Hirschmann	HiLCOS	BAT-R, BAT-F, BAT450-F, BAT867-R, BAT867-F, WLC, BAT Controller Virtual	HiLCOS 10.34.6464 (Release Update 8)

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 and https://garrettcom-support.belden.com.

Related Links

[1] https://ssd-disclosure.com/ssd-advisory-lancom-lcos-heap-overflow/

[2] https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C/CR:L/IR:L/AR:M/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:N/MI:N/MA:H&version=3.1

Disclaimer

Revisions

V1.0 (<2024-10-16>):	Bulletin released.
V1.0 (<2024-09-16>):	Bulletin created.