HTTP(S) Vulnerability in HiOS

Date: 2026-09-09
Version: 1.0

Summary

HiOS devices are affected by a vulnerability in the integrated web server. Due to missing validation of HTTP(S) content, specially crafted HTTP(S) requests to a specific endpoint may be processed incorrectly. This can cause the device to perform an unintended reboot. An attacker could exploit this vulnerability remotely, leading to a temporary denial-of-service condition and loss of availability for the affected device.

The severity is rated High with a CVSS v4 Score of 8.7.
(CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N)

Affected Products

Brand	Product Line	Affected Version(s)
Hirschmann	HiOS Switch Platform	07.1.11 and lower 09.0.12 and lower 08.7.09 and lower 09.3.02 and lower 10.3.07 and lower 10.4.00 and lower

Mitigation

Customers are advised to upgrade their devices to the following versions:

- 07.1.12 or higher
- 08.7.10 or higher
- 09.0.13 or higher
- 09.3.03 or higher
- 10.3.08 or higher
- 10.5.00 or higher

For Help or Feedback

To view all Belden Security Advisories or to report suspected security vulnerabilities, go to https://www.belden.com/security.
For technical support and other requests, please visit https://www.belden.com/support/technical-product-support-main.

Related Links

- Link to CVSS Calculator

Disclaimer

SUBJECT TO CHANGE WITHOUT NOTICE. BELDEN RESERVES THE RIGHT TO CHANGE OR UPDATE ADVISORIES AT ANY TIME.

Revisions

V1.0 2026-09- 04	Security Advisory created.