

Web Interface Vulnerability in HiOS

Date: 2025-10-09

Version: 1.0

Summary

A vulnerability has been identified in the HiOS Switch Platform where an HTTP GET request to a specific endpoint causes the device to perform a reboot.

The severity is rated Critical with a CVSS v3.1 score of 9.3. [1]

Affected Products

Brand	Product Line	Version(s)
Hirschmann	HiOS Switch Platform	Since 09.1.00

Mitigation

Hirschmann – HiOS Switch Platform

Update to version 09.4.05, 10.3.01 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

- [1] [CVSS v3.1 Score](#)

Disclaimer

THE SECURITY ADVISORY, AND INFORMATION CONTAINED HEREIN, ARE PROVIDED ON AN "AS IS" BASIS AND DO NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE ADVISORY, AND INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED FROM THE ADVISORY, IS AT YOUR OWN RISK. INFORMATION IN THIS ADVISORY AND ANY RELATED COMMUNICATIONS IS BASED ON OUR KNOWLEDGE AT THE TIME OF PUBLICATION AND IS SUBJECT TO CHANGE WITHOUT NOTICE. BELDEN RESERVES THE RIGHT TO CHANGE OR UPDATE ADVISORYS AT ANY TIME.

Revisions

V1.0 Advisory created.