

Web Server Authentication Bypass Vulnerability in HiEOS

Date: 2024-04-26

Version: 1.0

Executive Summary

A vulnerability in the HTTP(S) management module of HiEOS devices could allow an unauthenticated, remote attacker to bypass authentication for web server resources.

Details

The vulnerability is due to improper handling of authentication requests. An attacker could exploit this vulnerability by crafting specially formed HTTP(S) requests and incorrectly receive the authentication status and privileges.

The CVSS 3.1 score of this behavior is 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

Impact

An exploit could allow the attacker to execute administrative actions like configuration download/upload, changing the firmware or gain administrative access to the device.

Affected Products

Brand	Product Line / Platform	Product	Version
Hirschmann	HiEOS	LRS11	lower than 01.1.00

Solution

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

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>.

Disclaimer

THE SECURITY BULLETIN, 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 BULLETIN, AND INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED FROM THE BULLETIN, IS AT YOUR OWN RISK. INFORMATION IN THIS BULLETIN 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 BULLETINS AT ANY TIME.

Revisions

V1.0 (2024-04-26): Bulletin released.