Password Change Authentication Bypass Vulnerability in HiOS & HiSecOS

Date: 2021-05-11
Version: 1.0
References: CVE-2021-27734[1]

Executive Summary

Under some conditions, the HTTP(S) server does not correctly check whether a request to change a password is properly authenticated.

Details

The CVSS v3.1 severity of this vulnerability is 9.8 (critical):
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Impact

An attacker may change the password of any existing user.

Affected Products

Brand	Product Line / Platform	Product	Version
Hirschmann	HiOS	RSP, RSPE, RSPS, RSPL, MSP, EES, EESX, GRS, OS, RED	07.1.01, 07.1.02, 08.1.00 – 08.5.xx
Hirschmann	HiSecOS	EAGLE	03.3.00 or higher

Solution

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

Brand	Product Line / Platform	Product	Version
Hirschmann	HiOS	RSP, RSPE, RSPS, RSPL, MSP, EES, EESX, GRS, OS, RED	07.1.03 or higher, 08.6.00 or higher
Hirschmann	HiSecOS	EAGLE	04.1.00 or higher

Mitigation: Turn off the HTTP and HTTPS server or restrict access to both protocols to trusted IP addresses via the Restricted Management Access feature.

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://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27734

Disclaimer

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 (2021-05-11):	Bulletin published.