RADIUS Vulnerability in Multiple Products

Date: 2025-10-24
Version: 1.0

Summary

RADIUS Protocol under RFC 2865 is susceptible to forgery attacks by a local attacker who can modify any valid Response (Access-Accept, Access-Reject, or Access-Challenge) to any other response using a chosen-prefix collision attack against MD5 Response Authenticator signature.

The following vulnerability affects one or more versions of the products listed in the next section:

ID	Title / Description	Severity
CVE-2024-3596	RADIUS Protocol under RFC 2865 is susceptible to forgery attacks	CVSS v3.1: 9.0

Affected Products

Brand	Product Line	Affected Version(s)
Hirschmann	HiOS Switch Platform	All
Hirschmann	Classic Switch Platform	All
Hirschmann	HiLCOS Wireless Platform	10.34-RU7 and lower
Hirschmann	HiSecOS Firewall Platform	All
macmon	macmon-NAC	All
Hirschmann IT	Enterprise Managed Switches	All

Mitigation

Hirschmann – HiOS Switch, Classic Switch and HiSecOS Firewall Platforms

In the RADIUS default configuration products are not affected. If the RADIUS Server Message Authenticator option is disabled, the product is affected. We advise keeping this parameter in default state. The parameter can be configured via CLI and SNMP:

Classic Switch CLI: `radius server msgauth`
Classic Switch MIB: `hmAgentRadiusServerMsgAuth`

HiOS Switch / HiSecOS Firewall CLI: `radius server auth modify <index> msgauth`
HiOS Switch / HiSecOS Firewall MIB: `hm2AgentRadiusServerMsgAuth`

Hirschmann – HiLCOS Wireless Platform

Update to version 10.34-RU8

macmon – macmon-NAC

Until version 6.5.0, only the features “MAC authentication Bypass (MAB)” and “Switch Login” are affected, if the authenticator does not use the RADIUS attribute message authenticator.
In versions higher than 6.5.0 the new setting “`radius.require_message_authenticator`” must be enabled to force the usage of the RADIUS attribute message authenticator for “MAB” and “Switch Login”.

Hirschmann IT – Enterprise Managed Switches

To mitigate this vulnerability there are two options:

1) Enable EAP relay mode and add the Message-Authenticator attribute by configuring
   `dot1x eap-relay enable`
   on the interface performing 802.1X authentication.
2) Use the tacacs-group method for the authentication configuration

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] NVD: CVE-2024-3596

Disclaimer

Revisions

V1.0 (2025-10-24) Security Advisory published.