RADIUS authentication vulnerability

Date: February 26, 2018
Version: 1.0

Executive Summary

The login using HTTPS is vulnerable if the device is using RADIUS to check the user/password and a password longer than 128 characters is submitted.

Details

The HTTPS server on the device exposes an interface to login into the device. The interface receives a username and password combination. In case the given user is configured to be authenticated with a RADIUS server, the password will be copied into a local buffer with a fixed size of 128 bytes, allowing a buffer overflow attack.

Impact

Successful exploitation of the vulnerability may cause:

- Device crash (reboot)
- Execution of code if the request is modified accordingly

Affected Products

Brand	Product Line / Platform	Product	Version
Hirschmann	Classic Firewall	EAGLE, EAGLE One	05.3.02 and before

Solution

Update affected products to the following release that resolves this issue.

Brand	Product Line / Platform	Product	Version
Hirschmann	Classic Firewall	EAGLE, EAGLE One	05.3.03

The following workarounds can be used:

- Disable RADIUS for user authentication:
  - If RADIUS authentication is disabled for user authentication, the vulnerability is not exploitable.

- Allow web server access (login requests) from known IP addresses / network only or disable web service:
  - If the access to the web server can be restricted to known IP addresses and networks, the access from “outside”/”unknown” network can be avoided. Alternatively if you don’t need the web service you can disable the web server.

For Help or Feedback

To view all Belden Security Advisories and 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.eu.com

Disclaimer

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 (February 26, 2018): Bulletin published.