Potential false forward of IPv4 multicast / broadcast traffic by HiLCOS Layer-2 Firewall

Date: May 8, 2017
Version: 1.0

Executive Summary

In a certain configuration, the HiLCOS Layer-2 Firewall will forward IPv4 multicast and broadcast traffic, even when some filter rules are present to deny these packets. Belden recommends that its customers upgrade the software on the devices in question to a release that contains the solution. They can also apply the configuration workaround suggested below to the Layer-2 Firewall.

Details

The Layer-2 Firewall in HiLCOS software versions 9.10, 9.12 and 9.14 does not filter multicast and broadcast IPv4 packets correctly.
The Layer-2 Firewall offers the possibility to enable or disable filtering traffic directed to the device's management IP-address by checking or unchecking the corresponding checkbox. When this option is disabled, all configured filters for multicast traffic are not applied, so the corresponding IPv4 multicast and broadcast packets are not handled by the Layer-2 Firewall. As a result, the affected packets bypass the Layer-2 Firewall.

Impact

In case there is a multicast or broadcast based application present in the network, the related multicast packets might be bridged by the device unfiltered. Thus, a potential attacker who is able to get physical access to the wired or wireless network might inject or observe multicast or broadcast traffic.

Affected Products

Brand	Product Line / Platform	Product	Version
Hirschmann	HiLCOS	OpenBAT, BAT450, WLC	9.10.5126-REL, 9.12.5500-REL
		BAT867	9.14.5500-REL

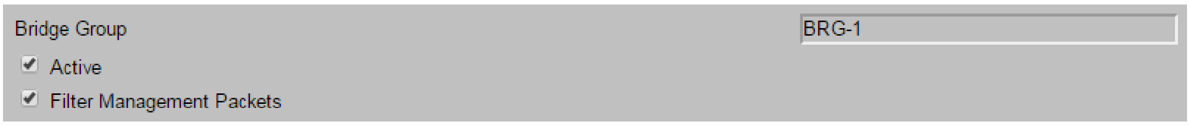
Solution

It is recommended to update devices running the affected software version to the following HiLCOS software version.

Brand	Product	Version	Links
Hirschmann	OpenBAT, BAT450, WLC	9.12.5600-RU1 or higher	[1]
	BAT867	9.14.5600-RU1 or higher	

Workaround

As a possible configuration workaround, it is recommended to activate the **Filter Management Packets** option, which activates the filter for packets directed to the device management IP address. This can be done in the LANconfig/WebIF dialogue "Configuration / Firwall-QoS / L2-Firewall / Bridge Group".



Bridge Group: BRG-1

☑ Active

☑ Filter Management Packets

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.

Related Links

- [1] Hirschmann Support Portal: https://hirschmann-support.belden.eu.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 (May 8, 2017):	Bulletin published.