IPsec Firewall Bypass Vulnerability in WLAN (HiLCOS) Products

Date: 2021-01-11
Version: 1.0
References: -

Executive Summary

Under certain conditions, traffic from a VPN might bypass the configured firewall rules.

Details

A potentially security-relevant issue has been fixed on OpenBAT/BAT450 products in conjunction with IPv6. This issue can occur when IPv6 networks are connected via IPSec (IKEv1 or IKEv2), and an IPv6 Internet connection is used simultaneously.

Impact

This vulnerability allows an attacker connected via IPSec to bypass firewall rules. Depending on the actual firewall rules, this may expose devices or networks to unwanted and potentially harmful traffic.

Affected Products

Brand	Product Line / Platform	Product	Version
Hirschmann	HiLCOS / BAT	OpenBAT, BAT450	8.80-REL, 8.90-REL, 9.00-REL, 9.00-RU1, 9.10-REL, 9.12-REL, 9.12-RU1, 9.12-RU2, 9.12-RU3, 9.12-RU4, 9.12-RU5, 9.12-RU6, 9.12-RU7, 9.12-RU8, 9.12-RU9, 9.13-REL, 9.13-RU1. 10.12-REL, 10.12-RU1

Solution

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

Brand	Product Line / Platform	Product	Version
Hirschmann	HiLCOS / BAT	OpenBAT, BAT450	10.12-RU2 or later

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.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 (2021-01-11):	Bulletin published.