pppd vulnerability in Hirschmann OWL devices

Date: 2020-05-27
Version: 1.0
References: CVE-2020-8597

Summary

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

ID	Title / Description	Severity
CVE-2020-8597	pppd (Point to Point Protocol Daemon) versions 2.4.2 through 2.4.8 are vulnerable to buffer overflow due to a flaw in Extensible Authentication Protocol (EAP) packet processing in eap_request and eap_response subroutines. Impact: By sending an unsolicited EAP packet to a vulnerable ppp client or server, an unauthenticated remote attacker could cause memory corruption in the pppd process, which may allow for arbitrary code execution.	CVSS v3.0: 9.8

Affected Products

Brand	Product Line / Platform	Product	Version
Hirschmann	Cellular Router	OWL (all models)	All prior to 06.2.04

Solution

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

Brand	Product Line / Platform	Product	Version
Hirschmann	Cellular Router	OWL (all models)	06.2.04

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.

Related Links

- https://nvd.nist.gov/vuln/detail/CVE-2020-8597

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 (2020-05-28):	Bulletin created.