Multiple dnsmasq vulnerabilities in OWL 3G, OWL LTE, and OWL LTE M12

Date: 2020-06-15
Version: 1.0
References: CVE-2017-14491, CVE-2017-14492, CVE-2017-13704

Summary

The following vulnerabilities affect the DNS and DHCP functionality in one or more versions of the products listed in the next section:

ID	Title / Description	Severity
CVE-2017-14491	Heap-based buffer overflow in dnsmasq before 2.78 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted DNS response.	CVSS v3.0: 9.8
CVE-2017-14492	Heap-based buffer overflow in dnsmasq before 2.78 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted IPv6 router advertisement request.	CVSS v3.0: 9.8
CVE-2017-13704	In dnsmasq before 2.78, if the DNS packet size does not match the expected size, the size parameter in a memset call gets a negative value. As it is an unsigned value, memset ends up writing up to 0xffffffff zero's (0xffffffffffffffff in 64 bit platforms), making dnsmasq crash.	CVSS v3.0: 7.5

Affected Products

Brand	Product Line / Platform	Product	Version
Hirschmann	OWL	OWL 3G, OWL LTE, OWL LTE M12	1.0.00, 1.1.00, 1.2.01, 1.2.04

Solution

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

Brand	Product Line / Platform	Product	Version
Hirschmann	OWL	OWL 3G, OWL LTE, OWL LTE M12	6.1.9 or higher

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://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-14491
- https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-14492
- https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-13704

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 (2020-06-15):	Bulletin created.