

Belden GarrettCom MNS 6K and 10K SNMP Vulnerability

Date: Aug 09, 2018

Version: 1.0

Summary

The following vulnerability affect the SNMP functionality in one or more versions of the Magnum 6K and 10K products listed in the next section:

ID	Title / Description	Severity
CVE-2018-1000116	SNMP Heap Corruption Vulnerability in UDP Protocol Handler that can result in command execution	CVSS v3.0: 9.8

Affected Products

Brand	Product Line / Platform	Product	Version
GarrettCom	Magnum Managed Switches	Magnum 6K and 10K	4.7.10 and earlier

Solution

Updates are available that address the vulnerabilities. Customers are advised to update their product to version 4.7.11 or later.

Brand	Product Line / Platform	Product	Version
GarrettCom	Magnum Managed Switches	Magnum 6K and 10K	4.7.11

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> and <https://garrettcom-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 (Aug 09, 2018): Bulletin created.