Belden GarrettCom MNS 6K and 10K Device Access and Security Key Vulnerabilities

Date: May 8, 2017
Version: 1.0

Executive Summary

Six issues have been identified in the Belden GarrettCom 6K and 10K series of managed switches. These issues fall into three categories:

- an unauthorized user can gain access to the device,
- an unprivileged but authenticated user can elevate their access to manager level,
- three weaknesses related to SSL and HTTP cyphers and keys.

Belden recommends that customers upgrade to firmware version 4.7.7 or later to mitigate these vulnerabilities.

Details

1. A certain hardcoded string can be used to bypass web authentication
2. Unprivileged but authenticated users can potentially elevate their access to manager level
3. Issuing a certain form of URL against the device's web server can lead to a buffer overflow in the HTTP Server which can can lead to memory corruption, possibly including remote code execution
4. Firmware version 4.6.0 devices use the same default SSL certificates and the documentation is not clear that users must install their own keys and certificates on the switch to override the default
5. The switches support a number of weak SSL ciphers such as 56-bit DES, RC4, MD5 based MACs
6. HTTP session key generation is weak

Impact

These vulnerabilities could potentially allow an unauthorized user to access the device or potentially to execute unwanted code.

Affected Products

Issue 1 affects the following products and software versions:

Brand	Product Line / Platform	Product	Version
GarrettCom	Magnum Managed Switches	Magnum 6K and 10K	4.6.0 and earlier

Issues 2-6 affect the following products and software versions:

Brand	Product Line / Platform	Product	Version
GarrettCom	Magnum Managed Switches	Magnum 6K and 10K	4.7.6 and earlier

Solution

For Issues 1-3, 5 and 6:
Update 6K and 10K products to version 4.7.7 or later to resolve these issues. 6K and 10K firmware releases are available at the GarrettCom support portal [1].

For Issue 4:
Refer to the User Manual and follow the section "Using Secure Web Server", under Chapter 3 to replace the default certificates with Keys and Certificates specific to user organization.

Deleted: 4

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://garrettcom-support.belden.eu.com.

Acknowledgments

Belden thanks David Tomaschik, Andrew Griffiths, and Xiaoran Wang of the Google Assessments team for identifying and reporting these issues and for working with us to help protect customers.

Related Links

[1] GarrettCom support portal: https://garrettcom-support.belden.eu.com

Disclaimer

Revisions

V1.0 (May 8, 2017): Bulletin published.

Deleted: April 21

Deleted: 4