Belden GarrettCom MNS 6K and 10K Security Keys, Embedded Password, Cross-site Scripting and Web Server DOS Vulnerabilities

Date: June 5, 2015
Version: 1.0
References: ICS-VU-017409

Executive Summary

Four issues have been identified in the Belden Garrettcom 6K and 10K series of managed switches falling in the area of SSL Key exposure, hard coded user account, Cross-site Scripting and a potential web-based DOS vulnerability. Belden Garrettcom has validated these vulnerabilities through testing and confirms that the issues affect the 10K and 6K product lines.

Belden recommends that its customers upgrade switch firmware to version 4.5.6 or later to mitigate these vulnerabilities. These vulnerabilities have been publicly disclosed.

Impact

1. It is possible for certain security keys of the Belden Garrettcom 10K and 6K products to be deciphered potentially posing a man-in-the-middle security threat when using HTTPS to communicate with the device.
2. The firmware contains a hardcoded password for a privileged user. While the user account for this user is actually not enabled in the operating switch, its appearance is deemed inappropriate.
3. Cross-site script vulnerabilities exist in the web server present on the device which can be exploited by an un-authenticated attacker.
4. By issuing a certain form of URL against the device's web server, memory corruption can occur which results in a reboot of the device.

Affected Products

Brand	Product Line / Platform	Product	Version
Garrettcom	Magnum 10K	10KT, 10KG	4.5.5 and lower
Garrettcom	Magnum 6K	6K32, 6K25, 6K16, 6K8, 6KL, 6KM, 6KQ	4.5.5 and lower

Solution

Update 6K and 10K products to version 4.5.6 or later to resolve these issues. 10K firmware releases are available at the firmware portal [1]. 6K firmware releases are available at the firmware portal [2].

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 the following for working with us to help protect customers:

- Ashish Kamble
- Eireann Leverett

Related Links

[1] 10K firmware portal: http://www.garrettcom.com/techsupport/sw_downloads_10kt.htm
[2] 6K firmware portal: http://www.garrettcom.com/techsupport/sw_downloads_6k.htm

Disclaimer

Revisions

V1.0 (June 5, 2015): Bulletin created.