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

<table>
<thead>
<tr>
<th>Brand</th>
<th>Product Line / Platform</th>
<th>Product</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>GarrettCom</td>
<td>Magnum 10K</td>
<td>10KT, 10KG</td>
<td>4.5.5 and lower</td>
</tr>
<tr>
<td>GarrettCom</td>
<td>Magnum 6K</td>
<td>6K32, 6K25, 6K16, 6K8, 6KL, 6KM, 6KQ</td>
<td>4.5.5 and lower</td>
</tr>
</tbody>
</table>

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


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 (June 5, 2015): Bulletin created.