

ICX35 User Interface Input Validation Issue

Date: May 8, 2017

Version: 1.0

Executive Summary

Several fields in the ICX35 web user interface accept system commands that can be used to gain root privileges to the device. The web UI can be accessed via the cellular network, so this vulnerability can be exploited remotely.

Details

During internal comprehensive penetration testing of the ICX35 cellular gateway, several fields in the web user interface were found to allow the entry of system commands with root privileges. This could allow an attacker to execute malicious commands on the ICX35 processor. Because the user interface is accessible over the cellular connection, this vulnerability could be exploited remotely.

Impact

An attacker could use this vulnerability to execute malicious commands on the ICX35 processor, using it as a platform for malicious code. The ICX35 provides Internet connectivity through its cellular WAN port, which means it could be used as a platform for a broad based attack.

Affected Products

Brand	Product Line / Platform	Product	Version
ProSoft Technology	Industrial Cellular Gateways	ICX35-HWC-x	1.0, 1.1, 1.1d, 1.2.x

Solution

This vulnerability has been fixed in firmware version 1.3, released on April 12, 2017. Users are encouraged to update the firmware on all ICX35 gateways to version 1.3 or later. Firmware can be updated through ProSoft Connect or by downloading the firmware files from the Downloads section of the ICX35 product web page: <http://www.prosoft-technology.com/Products/Industrial-Wireless/Intelligent-Cellular/Industrial-Cellular-Gateway-ICX35-HWC>

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 <http://www.prosoft-technology.com/About-Us/Contact-Us>.

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 (May 4, 2017): Bulletin published.