IOActive Security Advisory

Title	Turck BL20/BL67 Programmable Gateways undocumented hard-coded accounts
Severity	Critical - CVSS 10.0
Discovered by	Ruben Santamarta

Affected Products

- Turck BL20 and BL67 Programmable Gateways. All versions.

The affected products provide communication between the communications bus and I/O modules. According to TURCK, the BL20 and BL67 are deployed across several sectors. These include agriculture and food, automotive, and critical manufacturing. TURCK estimates that these products are used primarily in the United States and Europe with a small percentage in Asia.

Impact

This vulnerability allows an attacker to remotely access the device, via its embedded FTP server, by using the undocumented hard-coded credentials. Thus, the attacker can install a trojanized firmware to control communications and processes.

This malicious code may create false communication between remote I/Os, PLCs, or DCS systems in order to compromise additional devices, disrupt legitimate services, or alter industrial processes.

Technical Details

The static analysis of the firmware, which was performed via reverse engineering, revealed that certain hard-coded accounts are added to the internal authentication mechanism during the system initialization. These credentials can be used to remotely access the device via its FTP server, which is listening for connections on port 21.

Further technical details will be published in our blog soon.

Reserved CVE Number: CVE-2012-4697

Solution

TURCK has provided a firmware update for these products. The firmware update mitigates the vulnerability by removing the hard-coded accounts accessible by the FTP service.

References:

http://ics-cert.us-cert.gov/advisories/ICSA-13-136-01