PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Telefon: +49 5235 300
Telefax: +49 5235 3-41200
Internet: http://www.phoenixcontact.com
USt-Id-Nr.: DE124613250
WEEE-Reg.-Nr.: DE50738265

PHOENIX CONTACT GmbH & Co. KG · 32825 Blomberg

17 November 2017
S1: 300385654

Security Advisory for FL COMSERVER products [CVE-2017-16723]

Synopsis

Cross-site Scripting (XSS) vulnerability in FL COMSERVER products

Affected products

FL COMSERVER products with firmware prior 1.99, 2.20 or 2.40

Order No	Description	New Firmware	Generation
2313478	FL COMSERVER BASIC 232/422/485	2.40	2nd Generation
2313452	FL COMSERVER UNI 232/422/485	2.40	
2904681	FL COMSERVER BAS 232/422/485-T	2.40	
2904817	FL COMSERVER UNI 232/422/485-T	2.40	
2744490	FL COM SERVER RS232	1.99	1st Generation
2708740	FL COM SERVER RS485	1.99	
2313300	PSI-MODEM/ETH	2.20	

Issue

On devices with older firmware versions, an unauthenticated user with network access is able to change (but not activate) the configuration variables by accessing a specific URL on the web server, without authenticating in the web interface first. A changed configuration can only be permanently saved and activated by an authenticated user. However, since the input is not properly sanitised, an attacker could inject malicious JavaScript code. When this code is executed on the client of an authenticated user, changed configuration variables could be saved and activated without user interaction.

Details

The webserver of the devices does not sufficiently exclude JavaScript code, allowing execution of JavaScript code on the Client.

Mitigation

Customers using the devices in an unprotected network environment are recommended to update the device firmware to the firmware versions mentioned in the table above which fixes this vulnerability.