Process - Informatik Entwicklungsgesellschaft mbH

AUTOMATISIERUNG + GASANALYSE + VERFAHRENSTECHNIK + STEUERUNGSTECHNIK

AEG, BOSCH, KLÖCKNER-MOELLER, MITSUBISHI, SIEMENS S5 / S7
INDUSTRIELLE NETZWERK- UND SICHERHEITSTECHNIK, FUNKVERBINDUNGEN
FERNWARTUNG, INTERFACEKABEL, SPEICHERMODULE, DIAGNOSE-SYSTEM
PROGRAMMIER-SOFTWARE, KOMMUNIKATIONS-TREIBER, SCHNITTSTELLEN-VERDOPPLER
SAUERSTOFFANALYSE, HAERTEREITECHNIK, LEITSYSTEME, GUTACHTEN
ENTWICKLUNG, PRODUKTION, VERTRIEB UND TECHNISCHER SUPPORT

Process-Informatik GmbH • Im Gewerbegebiet 1 • 73116 Wäschenbeuren • Germany

Security Advisory 2015/12/02
2015/12/02 – Process-Informatik Entwicklungsgesellschaft mbH

Analyzesed by
SCADACS (Freie Universität Berlin)
FEST AG
We thank the authors:
Johannes Klick, Matthias Sekul, Stephan Lau, Daniel Marzin

Synopsis
security lacks in WEB-Gui on S7-Firewall / TeleRouter

Issue
1. the WEB-GUI doesn't support https
2. Security flaw in the webgui of the device which allows execution of malicious code in the context of the user's browser session.
3. Security flaw in the authentication of the web server, which allows replay attacks even after log off and reboot.

Impact
1. An attacker can read along the communication between WEB-GUI and webbrowser.
2. The web gui does not properly encode output of user data in most fields. Exploiting this vulnerability leads to stored cross-site scripting (XSS) and allows execution of JavaScript code.
3. The web server uses digest access for authentication. Digest access authentication is one of the agreed-upon methods a web server can use to negotiate credentials. How ever it is not properly implemented, so the nonce can be used multiple times.

Affected products
S7-Firewall / TeleRouter
- all models with OS version older than V 1.09
- all models with firmware version older than 1.84

Solution
Get information of OS / Firmwareversion installed . (Top menu: Info)
If OS Version older than V1.09 is installed, install OS V1.09, where firmware version V1.85 or newer is included (see product downloads on our site).
In OS Version V1.09 or newer, Firmwareversion V1.85 or newer is included by default