**Pressemitteilung**

# Hoch-kritische Sicherheitslücke in S7 Software identifiziert

Speicherprogrammierbare Steuerung S7-1200

Sankt Augustin, 7. Januar 2013

Die IT-Sicherheitsberatung softScheck GmbH hat eine bisher nicht-erkannte kritische Sicherheitslücke (**Zero-Day-Vulnerability**) mit Fuzzing identifiziert, sie beschrieben und auch Behebungsvorschläge erarbeitet. Die Informationen wurden entsprechend der softScheck-internen Security Vulnerability Reporting Policy entgeltfrei der Siemens AG zur Verfügung gestellt:

http://www.siemens.com/corporate-technology/pool/de/forschungsfelder/siemens_security_advisory_ssa-724606.pdf

und

http://www.industry.siemens.com/topics/global/de/industrial-security/news-alerts/alerts/seiten/alert-201212a.aspx

Diese Sicherheitslücke ist auf einer Speicherprogrammierbaren Steuerung (Programmable Logic Controller – PLC) präsentierbar und kann mit einem Exploit ausgenutzt werden; sie ist von Siemens als hoch-kritisch mit CVSS Overall Score 7.0 (AV:N/AC:L/Au:N/C:N/I:N/A:C/E:POC/RL:U/RC:C) bewertet, weil Denial-of-Service Angriffe geführt werden können, die zum vollständigen Ausfall industrieller Prozesse führen.

Das **BSI und das ICS-CERT warnen vor zunehmenden Angriffen auf Industriesteuerungen**, speicherprogrammierbare Steuerungen / Programmable Logic Controller (SPS/PLC). Allein mit dem Verfahren Dynamic Analysis: Fuzzing wurden von softScheck in einer Stichprobe aus 15 Projekten aus dem Bereich Industriesteuerungsanlagen 100 hoch-kritische, bisher nicht-erkannte Sicherheitslücken identifiziert. Das BSI listet die konkreten Bedrohungen: „Industrial Control System Security - Top 10 Bedrohungen“ (ICSS-Top 10). Die von softScheck eingesetzten Verfahren werden u.a. vom Bundesamt für Informationssicherheit (BSI) unterstützt.

## Über softScheck

Die softScheck GmbH hat sich in den letzten Jahren als Alleinstellungsmerkmal in Europa mit der kostengünstigen Identifizierung bisher nicht-erkannter Sicherheitslücken (**Zero-Day-Vulnerabilities**) in jeder Art Software (und auch Hardware) neue, attraktive Wachstumsfelder erschlossen: In Anwendungssoftware (Webapplications, ERP, ERM, CRM, SCM, E-Business, CIM etc.) und Netzwerk-Protokollen, Embedded Systems und Industrial Control Systems (ICS), Manufacturing Execution Systems - Produktionsleitsysteme mit MES, SCADA (Leittechnik und –systeme), SPS bis zur Feldebene, im Smart Grid (z.B. Smart Meter Gateway), Cyber Physical Systems, M2M, Industrie 4.0, in Apps und Applets für smart and mobile Devices, im Cloud Computing und auch in Hardware.

softScheck führt regelmäßig **Sicherheitsprüfungen** von Software und Hardware durch. Daneben bietet softScheck selbstverständlich auch die klassische IT-Sicherheitsberatung an vom Grundschutz (ISO 27000-Familie) bis hin zur Hochsicherheit in der Informationsverarbeitung (Redundanz und Diversität) – auch mit Consulting, Coaching und Forensics.

## Kontakt:


Anja Wallikewitz
Tel.: 02241 – 255 43 – 11
Fax: 02241 – 255 43 – 29
anja.wallikewitz@softScheck.com

softScheck GmbH
Bonner Straße 108
53757 Sankt Augustin
www.softScheck.com