SSA-456423: Vulnerabilities in SIMATIC S7-1500 CPU family

Publication Date:	2014-03-12
Last Update:	2020-02-10
Current Version:	V1.1
CVSS v3.1 Base Score:	8.8

SUMMARY

The new firmware update for the SIMATIC S7-1500 CPU firmware fixes several vulnerabilities, which may have been exploitable via network by Web application attacks or Denial-of-Service attacks with specially crafted network packets on different ports.

Siemens addresses and fixes all of these issues by the new firmware update.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions < V1.5	Update to V1.5 http://support.automation.siemens.com/WW/view/en/88613339

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any specific mitigations or workarounds.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals.

Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

Products of the SIMATIC S7-1500 CPU family have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

SIPLUS extreme products are designed for reliable operation under extreme conditions and are based on SIMATIC, LOGO!, SITOP, SINAMICS, SIMOTION, SCALANCE or other devices. SIPLUS devices use the same firmware as the product they are based on.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2014-2249

The web server of the affected PLCs (port 80/tcp and port 443/tcp) might allow CSRF (Cross-Site Request Forgery) attacks, compromising integrity and availability of the affected device.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-352: Cross-Site Request Forgery (CSRF)

Vulnerability CVE-2014-2246

The integrated web server (port 80/tcp and port 443/tcp) of the affected device might be vulnerable to Cross-Site Scripting (XSS) attacks.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:T/RC:C
CWE	CWE-712: OWASP Top Ten 2007 Category A1 - Cross Site Scripting (XSS)

Vulnerability CVE-2014-2247

The integrated web server (port 80/tcp and port 443/tcp) of the affected device might allow attackers to inject HTML headers.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-113: Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting')

Vulnerability CVE-2014-2251

Due to low entropy in its random number generator, the authentication of the integrated web server (port 80/tcp and port 443/tcp) of S7-1500 PLCs might allow attackers to hijack web sessions over the network without authentication.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-331: Insufficient Entropy

Vulnerability CVE-2014-2248

The integrated web server (port 80/tcp and port 443/tcp) of the affected device might allow attackers to redirect users to untrusted websites.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-601: URL Redirection to Untrusted Site (‘Open Redirect’)

Vulnerability CVE-2014-2259

Specially crafted packets sent on port 443/tcp (HTTPS) might cause the device to go into defect mode. A cold restart is required to recover the system.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2014-2253

Specially crafted Profinet packets sent to the affected device might cause the device to go into defect mode. A cold restart is required to recover the system. The attacker must have access to the local Ethernet segment.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2014-2255

Specially crafted packets sent on port 80/tcp (HTTP) might cause the device to go into defect mode. A cold restart is required to recover the system.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2014-2257

Specially crafted packets sent on port 102/tcp (ISO-TSAP) might cause the device to go into defect mode. A cold restart is required to recover the system.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Dmitry Serebryannikov, Ilya Karpov, Alexey Osipov, Yury Goltsev, and Alex Timorin from Positive Technologies for coordinated disclosure
- Artem Zinenko from Kaspersky for pointing out that SIPLUS should also be mentioned

ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2014-03-12):	Publication Date
V1.1 (2020-02-10):	SIPLUS devices now explicitly mentioned in the list of affected products

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.