SSA-456423: Vulnerabilities in SIMATIC S7-1500 CPU

Publication Date 2014-03-12
Last Update 2014-03-12
Current Version V1.0
CVSS Overall Score 6.5

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
- 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

- SIMATIC S7-1500 CPU family: all versions < V1.5

DESCRIPTION

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

In the SIMATIC S7-1500 CPU firmware multiple vulnerabilities were discovered. The vulnerabilities allowed attackers to perform Denial of Service attacks with specially crafted HTTP(S), ISO-TSAP, or Profinet network packets. The integrated web server was also vulnerable to Cross-Site Request Forgery, Cross-Site Scripting, header injection, and open redirect attacks as well as privilege escalation. The vulnerabilities might have been exploited over the network without authentication.

Detailed information about the vulnerabilities is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSSv2 scoring system (http://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.

Vulnerability 1 (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 Base Score 5.8
CVSS Temporal Score 4.5
CVSS Overall Score 4.5 (AV:N/AC:M/Au:N/C:N/I:P/A:P/E:POC/RL:OF/RC:C)

Vulnerability 2 (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 Base Score 4.3
CVSS Temporal Score 3.4
CVSS Overall Score 3.4 (AV:N/AC:M/Au:N/C:N/I:P/A:N/E:POC/RL:OF/RC:C)

Vulnerability 3 (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 Base Score	5.8
CVSS Temporal Score	4.5
CVSS Overall Score	4.5 (AV:N/AC:M/Au:N/C:N/I:P/A:P/E:POC/RL:OF/RC:C)

Vulnerability 4 (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 Base Score	8.3
CVSS Temporal Score	6.5
CVSS Overall Score	6.5 (AV:N/AC:M/Au:N/C:P/I:P/A:C/E:POC/RL:OF/RC:C)

Vulnerability 5 (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 Base Score	4.3
CVSS Temporal Score	3.4
CVSS Overall Score	3.4 (AV:N/AC:M/Au:N/C:N/I:P/A:N/E:POC/RL:OF/RC:C)

Vulnerability 6 (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 Base Score	7.8
CVSS Temporal Score	6.1
CVSS Overall Score	6.1 (AV:N/AC:L/Au:N/C:N/I:N/A:C/E:POC/RL:OF/RC:C)

Vulnerability 7 (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 Base Score	6.1
CVSS Temporal Score	4.8
CVSS Overall Score	4.8 (AV:A/AC:L/Au:N/C:N/I:N/A:C/E:POC/RL:OF/RC:C)

Vulnerability 8 (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 Base Score	7.8
CVSS Temporal Score	6.1
CVSS Overall Score	6.1 (AV:N/AC:L/Au:N/C:N/I:N/A:C/E:POC/RL:OF/RC:C)

Vulnerability 9 (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 Base Score	7.8
CVSS Temporal Score	6.1
CVSS Overall Score	6.1 (AV:N/AC:L/Au:N/C:N/I:N/A:C/E:POC/RL:OF/RC:C)

Mitigating factors:

For vulnerability 1, 2, 3 and 5 the attacker must trick users of the devices to open malicious web pages. Usage of modern browsers may reduce the probability of successful exploitation.

For vulnerability 7 the attacker must have access to the local Ethernet segment.

All other vulnerabilities require network access to the port.

Siemens recommends operating the devices only within trusted networks [3].

SOLUTION

Siemens provides firmware update V1.5.0 [1] which fixes the potential vulnerabilities.

As a general security measure Siemens strongly recommends to protect network access to S7-1500 CPUs with appropriate mechanisms. It is advised to follow recommended security practices [5] and to configure the environment according to operational guidelines [2] in order to run the devices in a protected IT environment.

ACKNOWLEDGEMENT

Siemens thanks the following for their support and efforts:

- Dmitry Serebryannikov, Ilya Karpov, Alexey Osipov, Yury Goltsev, Alex Timorin, Alexey Osipov, Ilya Karpov from Positive Technologies for coordinated disclosure of vulnerabilities 2, 3, 4, and 5.

ADDITIONAL RESOURCES

[1] The firmware update can be obtained here:
http://support.automation.siemens.com/WW/view/en/88613339

[2] An overview of the operational guidelines for Industrial Security (with the cell protection concept):
http://www.industry.siemens.com/topics/global/en/industrial-security/Documents/operational_guidelines_industrial_security_en.pdf

[3] Information about Industrial Security by Siemens:
http://www.siemens.com/industrialsecurity

[4] Recommended security practices by ICS-CERT:
http://ics-cert.us-cert.gov/content/recommended-practices

[5] For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:
http://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2014-03-12): Publication Date

DISCLAIMER

See: http://www.siemens.com/terms_of_use