SSA-654382: Vulnerabilities in SIMATIC S7-1200 CPU

Publication Date 2014-03-20
Last Update 2014-04-15
Current Version V1.2
CVSS Overall Score 6.5

Summary:

The latest product release of the SIMATIC S7-1200 CPU fixes several vulnerabilities. The most severe of these vulnerabilities could allow an attacker to take over an authenticated web session if the session token can be predicted. The attacker must have network access to the device to exploit this vulnerability.

Further vulnerabilities resolved in this product release are discussed below.

AFFECTED PRODUCTS

- SIMATIC S7-1200 CPU family: V2.X and V3.X

DESCRIPTION

Products in the Siemens SIMATIC S7-1200 PLC family have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

Six vulnerabilities have been resolved in the latest product release. 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 integrated web server (port 80/tcp and port 443/tcp) of the affected PLCs could allow CSRF (Cross-Site Request Forgery) attacks, compromising integrity and availability of the affected device, if social engineering is used to cause an unsuspecting user to click on a malicious link.

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-2014-2258)

An attacker could cause the device to go into defect mode if specially crafted packets are sent to port 443/tcp (HTTPS). 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 3 (CVE-2014-2250)

Due to low entropy in its random number generator, the integrated web server's authentication method (port 80/tcp and port 443/tcp) could allow attackers to hijack web sessions over the network if the session token can be predicted.

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 4 (CVE-2014-2252)

An attacker could cause the device to go into defect mode if specially crafted PROFINET packets are sent to the device. A cold restart is required to recover the system.

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 5 (CVE-2014-2254)

An attacker could cause the device to go into defect mode if specially crafted packets are sent to port 80/tcp (HTTP). 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 6 (CVE-2014-2256)

An attacker could cause the device to go into defect mode if specially crafted packets are sent to port 102/tcp (ISO-TSAP). 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 use of modern browsers reduces the probability of successful exploitation. For vulnerability 4 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 [2].

SOLUTION

Siemens provides the SIMATIC S7-1200 CPU product release V4.0 [1] which fixes these vulnerabilities.

As a general security measure Siemens strongly recommends to protect network access to S7-1200 CPUs with appropriate mechanisms. It is advised to follow recommended security practices [4] 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:

- Ralf Spenneberg from OpenSource Training for coordinated disclosure of vulnerability 2.
- Alexander Timorin, Alexey Osipov from Positive Technologies for coordinated disclosure of vulnerabilities 3 and 4.

- Lucian Cojocar and Jonas Zaddach from EURECOM for coordinated disclosure of vulnerability 5.
- Sascha Zinke from the FU Berlin's work team SCADACS for coordinated disclosure of vulnerability 6.

ADDITIONAL RESOURCES

[1] Siemens product release V4.0 firmware requires the use of S7-1200 V4.0 CPU hardware. Further details on the S7-1200 V4.0 release can be found here: http://support.automation.siemens.com/WW/view/en/86567043

[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 (2014-03-20): Publication Date
V1.1 (2014-03-25): Updated Section Acknowledgment
V1.2 (2014-04-15): Updated Affected Products

DISCLAIMER