SSA-279823: Cross-Site Scripting vulnerability in the SIMATIC S7-1200 CPU family

Publication Date: 2012-10-08
Last Update: 2020-02-10
Current Version: V1.1
CVSS v3.1 Base Score: 8.8

SUMMARY

Siemens SIMATIC S7-1200 CPUs, version 2 and higher, are capable of running an embedded web server. Web server functionality is disabled by default in the 1200 project configuration. However, if enabled, the web server is susceptible to Cross-Site Scripting (XSS). Siemens provides a firmware update which fixes this XSS vulnerability.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC S7-1200 CPU family (incl. SIPLUS variants): V2.x, V3.0.0 and V3.0.1	Update to V3.0.2 The firmware update can be obtained by contacting your Technical Support in your region (Germany:+49 911 895 7222, Americas:+1 423 262 5710, Asia-Pacific:+86 10 6475 7575)

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Disable JavaScript within the web browser used to access the S7-1200 web server
- Utilize a modern web browser with integrated XSS filtering mechanisms
- Deactivate the S7-1200 web server wherever possible

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 S7-1200 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 SVE-2012-0004

The web application does not filter user input in a way that prevents Cross-Site Scripting. If a user is enticed into passing specially crafted, malicious input to the S7-1200 web application via an HTTP request (e.g. by clicking on a malicious URL with embedded JavaScript), then JavaScript code can be returned and may then be executed by the user's browser. Various actions could be triggered by running malicious JavaScript code, including: modification of browser content delivered from the PLC; stealing data, such as session cookies; or issuing commands in the guise of the user to the PLC's web server.

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-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Dmitriy Serebryannikov, Artem Chaikin, Yury Goltsev, and Timur Yunusov 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 (2012-10-08): Publication Date
V1.1 (2020-02-10): SIPLUS devices now explicitly mentioned in the list of affected products

TERMS OF USE