# SSA-892012: Web Vulnerabilities in SIMATIC S7-1200 CPU Family

Publication Date: 2014-04-24
Last Update: 2020-02-10
Current Version: V1.1
CVSS v3.1 Base Score: 5.4

## SUMMARY

The latest product release of the SIMATIC S7-1200 CPU fixes two vulnerabilities. The more severe of these vulnerabilities could allow an attacker to inject HTTP headers if unsuspecting users are tricked to click on a malicious link.

Another vulnerability resolved in this product release is discussed below.

## AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|---|---|
| SIMATIC S7-1200 CPU family (incl. SIPLUS variants):<br>V2.X and V3.X | SIMATIC S7-1200 CPU product release V4.0 (V4.0 firmware requires the use of S7-1200 V4.0 CPU hardware)<br>https://support.industry.siemens.com/cs/ww/en/view/86567043 |

## WORKAROUNDS AND MITIGATIONS

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

- Operate the device only within trusted networks

## 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 CVE-2014-2908

The integrated web server (port 80/tcp and port 443/tcp) of the affected devices could allow Cross-Site Scripting (XSS) attacks if unsuspecting users are tricked to click on a malicious link.

| | |
|---|---|
| CVSS v3.1 Base Score | 4.3 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C |
| CWE | CWE-113: Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting') |

### Vulnerability CVE-2014-2909

The integrated web server (port 80/tcp and port 443/tcp) of the affected devices could allow attackers to inject HTTP headers if unsuspecting users are tricked to click on a malicious link.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.4 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L/E:P/RL:O/RC:C |
| CWE | CWE-113: Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting') |

## ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Ralf Spenneberg, Hendrik Schwartke and Maik Brüggemann from OpenSource Training 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 (2014-04-24): | 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.