SSA-478960: Missing CSRF Protection in the Web Server Login Page of Industrial Controllers

Publication Date: 2022-11-08
Last Update: 2022-11-08
Current Version: V1.0
CVSS v3.1 Base Score: 6.5

SUMMARY

The web server login page of affected products does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack..

Siemens has released updates for several affected products and recommends to update to the latest versions. Siemens is preparing further updates and recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC Drive Controller family: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC ET 200pro IM154-8 PN/DP CPU (6ES7154-8AB01-0AB0): All versions < V3.2.19	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/47354502/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200pro IM154-8F PN/DP CPU (6ES7154-8FB01-0AB0): All versions < V3.2.19	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/47354578/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200pro IM154-8FX PN/DP CPU (6ES7154-8FX00-0AB0): All versions < V3.2.19	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/62612377/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200S IM151-8 PN/DP CPU (6ES7151-8AB01-0AB0): All versions < V3.2.19	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/47353723/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200S IM151-8F PN/DP CPU (6ES7151-8FB01-0AB0): All versions < V3.2.19	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/47354354/ See further recommendations from section Workarounds and Mitigations

SIMATIC PC Station: All versions >= V2.1	Currently no fix is planned Disable the web server. Note that this feature is disabled by default See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 314C-2 PN/DP (6ES7314-6EH04-0AB0): All versions < V3.3.19	Update to V3.3.19 or later version https://support.industry.siemens.com/cs/ww/en/view/51466769/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 315-2 PN/DP (6ES7315-2EH14-0AB0): All versions < V3.2.19	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/40360647/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 315F-2 PN/DP (6ES7315-2FJ14-0AB0): All versions < V3.2.19	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/40944925/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 315T-3 PN/DP (6ES7315-7TJ10-0AB0): All versions < V3.2.19	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/85049260/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 317-2 PN/DP (6ES7317-2EK14-0AB0): All versions < V3.2.19	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/40362228/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 317F-2 PN/DP (6ES7317-2FK14-0AB0): All versions < V3.2.19	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/40945128/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 317T-3 PN/DP (6ES7317-7TK10-0AB0): All versions < V3.2.19	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/85059804/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 317TF-3 PN/DP (6ES7317-7UL10-0AB0): All versions < V3.2.19	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/85063017/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 319-3 PN/DP (6ES7318-3EL01-0AB0): All versions < V3.2.19	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/44442927/ See further recommendations from section Workarounds and Mitigations

SIMATIC S7-300 CPU 319F-3 PN/DP (6ES7318-3FL01-0AB0): All versions < V3.2.19	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/44443101/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC S7-1200 CPU family (incl. SIPLUS variants): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 Software Controller: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC S7-PLCSIM Advanced: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC WinCC Runtime Advanced: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SINUMERIK ONE: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIPLUS ET 200S IM151-8 PN/DP CPU (6AG1151-8AB01-7AB0): All versions < V3.2.19	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/47353723/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200S IM151-8F PN/DP CPU (6AG1151-8FB01-2AB0): All versions < V3.2.19	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/47354354/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-300 CPU 314C-2 PN/DP (6AG1314-6EH04-7AB0): All versions < V3.3.19	Update to V3.3.19 or later version https://support.industry.siemens.com/cs/ww/en/view/51466769/ See further recommendations from section Workarounds and Mitigations

SIPLUS S7-300 CPU 315-2 PN/DP (6AG1315-2EH14-7AB0): All versions < V3.2.19	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/40360647/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-300 CPU 315F-2 PN/DP (6AG1315-2FJ14-2AB0): All versions < V3.2.19	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/40944925/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-300 CPU 317-2 PN/DP (6AG1317-2EK14-7AB0): All versions < V3.2.19	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/40362228/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-300 CPU 317F-2 PN/DP (6AG1317-2FK14-2AB0): All versions < V3.2.19	Update to V3.2.19 or later version https://support.industry.siemens.com/cs/ww/en/view/40945128/ See further recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

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

- Do not access the product's web service via URLs coming from untrusted sources
- Disable the web server if possible

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

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

SIMATIC Drive Controllers have been designed for the automation of production machines, combining the functionality of a SIMATIC S7-1500 CPU and a SINAMICS S120 drive control.

SIMATIC PC Station is a software component that manages the SIMATIC software products and interfaces on a PC.

SIMATIC S7-1200 CPU products have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

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

SIMATIC S7-1500 Software Controller is a SIMATIC software controller for PC-based automation solutions.

SIMATIC S7-300 controllers have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

SIMATIC S7-400 controllers have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

SIMATIC S7-PLCSIM Advanced simulates S7-1200, S7-1500 and a few other PLC derivatives. Includes full network access to simulate the PLCs, even in virtualized environments.

SIMATIC WinAC RTX is a SIMATIC software controller for PC-based automation solutions.

SIMATIC WinCC Runtime Advanced is a visualization runtime platform used for operator control and monitoring of machines and plants.

SINUMERIK ONE is a digital-native CNC system with an integrated SIMATIC S7-1500 CPU for automation.

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-2022-30694

The login endpoint /FormLogin in affected web services does not apply proper origin checking.

This could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-352: Cross-Site Request Forgery (CSRF)

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- K Narahari from Sectrio for reporting the vulnerability

ADDITIONAL INFORMATION

SINUMERIK ONE: This vulnerability affects the integrated SIMATIC S7-1500 CPU.

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 (2022-11-08): Publication Date

TERMS OF USE