SSA-482956: Information Disclosure Vulnerability in SIMOTION before V5.5

Publication Date: 2023-06-13
Last Update: 2023-06-13
Current Version: V1.0
CVSS v3.1 Base Score: 4.6

SUMMARY

SIMOTION contains an information disclosure vulnerability that could allow an unauthenticated attacker to extract confidential technology object (TO) configuration from the device.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMOTION C240 (6AU1240-1AA00-0AA0): All versions >= V5.4 < V5.5 SP1	Update to V5.5 SP1 or later version https://support.industry.siemens.com/cs/ww/en/view/109812773/ See recommendations from section Workarounds and Mitigations
SIMOTION C240 PN (6AU1240-1AB00-0AA0): All versions >= V5.4 < V5.5 SP1	Update to V5.5 SP1 or later version https://support.industry.siemens.com/cs/ww/en/view/109812773/ See recommendations from section Workarounds and Mitigations
SIMOTION D410-2 DP (6AU1410-2AA00-0AA0): All versions >= V5.4 < V5.5 SP1	Update to V5.5 SP1 or later version https://support.industry.siemens.com/cs/ww/en/view/109812773/ See recommendations from section Workarounds and Mitigations
SIMOTION D410-2 DP/PN (6AU1410-2AD00-0AA0): All versions >= V5.4 < V5.5 SP1	Update to V5.5 SP1 or later version https://support.industry.siemens.com/cs/ww/en/view/109812773/ See recommendations from section Workarounds and Mitigations
SIMOTION D425-2 DP (6AU1425-2AA00-0AA0): All versions >= V5.4 < V5.5 SP1	Update to V5.5 SP1 or later version https://support.industry.siemens.com/cs/ww/en/view/109812773/ See recommendations from section Workarounds and Mitigations
SIMOTION D425-2 DP/PN (6AU1425-2AD00-0AA0): All versions >= V5.4 < V5.5 SP1	Update to V5.5 SP1 or later version https://support.industry.siemens.com/cs/ww/en/view/109812773/ See recommendations from section Workarounds and Mitigations

SIMOTION D435-2 DP (6AU1435-2AA00-0AA0): All versions >= V5.4 < V5.5 SP1	Update to V5.5 SP1 or later version https://support.industry.siemens.com/cs/ww/en/view/109812773/ See recommendations from section Workarounds and Mitigations
SIMOTION D435-2 DP/PN (6AU1435-2AD00-0AA0): All versions >= V5.4 < V5.5 SP1	Update to V5.5 SP1 or later version https://support.industry.siemens.com/cs/ww/en/view/109812773/ See recommendations from section Workarounds and Mitigations
SIMOTION D445-2 DP/PN (6AU1445-2AD00-0AA0): All versions >= V5.4	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMOTION D445-2 DP/PN (6AU1445-2AD00-0AA1): All versions >= V5.4 < V5.5 SP1	Update to V5.5 SP1 or later version https://support.industry.siemens.com/cs/ww/en/view/109812773/ See recommendations from section Workarounds and Mitigations
SIMOTION D455-2 DP/PN (6AU1455-2AD00-0AA0): All versions >= V5.4 < V5.5 SP1	Update to V5.5 SP1 or later version https://support.industry.siemens.com/cs/ww/en/view/109812773/ See recommendations from section Workarounds and Mitigations
SIMOTION P320-4 E (6AU1320-4DE65-3AF0): All versions >= V5.4	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMOTION P320-4 S (6AU1320-4DS66-3AG0): All versions >= V5.4	Currently no fix is planned See 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:

- Restrict physical access to the device and avoid using Security Level Low (eg. Service Selector Switch in position 8, with simotion.ini or the PSTATE program - see Section 3.5 of SIMOTION IT - SIMOTION IT Diagnostics and Configuration Manual) in production environments

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

SIMOTION is a scalable high performance hardware and software system for motion control.

SIMOTION P320 is an Industrial PC for motion control.

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-2023-27465

When operated with Security Level Low the device does not protect access to certain services relevant for debugging. This could allow an unauthenticated attacker to extract confidential technology object (TO) configuration from the device.

CVSS v3.1 Base Score	4.6
CVSS Vector	CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-213: Exposure of Sensitive Information Due to Incompatible Policies

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 (2023-06-13): Publication Date

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.