SSA-563922: Local Privilege Escalation Vulnerability in SIMOTION Tools

Publication Date:	2025-09-09
Last Update:	2025-09-09
Current Version:	V1.0
CVSS v3.1 Base Score:	8.1

SUMMARY

Several tools for the SIMOTION system are affected by a local privilege escalation vulnerability. This could allow an attacker to execute arbitrary code with SYSTEM privileges when a legitimate user installs an application that uses the affected setup component. This vulnerability poses a risk only during setup and installation phase of the affected tools.

Siemens is preparing fix versions and recommends specific countermeasures for products where fixes are not, or not yet available.

KNOWN AFFECTED PRODUCTS

Affected Product and Versions	Remediation
SIMATIC Technology Package TPCamGen (6ES7823-0FE30-1AA0): All versions affected by CVE-2025-43715	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMOTION OA MIIF (6AU1820-3DA20-0AB0): All versions affected by CVE-2025-43715	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMOTION OACAMGEN (6AU1820-3EA20-0AB0): All versions affected by CVE-2025-43715	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMOTION OALECO (6AU1820-3HA20-0AB0): All versions affected by CVE-2025-43715	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMOTION OAVIBX (6AU1820-3CA20-0AB0): All versions affected by CVE-2025-43715	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:

- Ensure that no other users are logged in and that no unknown programs are running before starting the installation of the affected products

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 Technology Package TPCamGen is part of the software package SIMATIC SimaPressServo. It determines optimized motion profiles for servo presses in which the tool is connected to the drive axis via a connecting rod.

SIMOTION OA MIIF is a SIMOTION tool that enables access to the variables of SIMOTION via a client.

SIMOTION OACAMGEN is a SIMOTION tool for cam generation with calculation of optimized motion profiles for servopresses.

SIMOTION OALECO is a SIMOTION tool for elimination of the position error resulting from cyclic distortion during a production process.

SIMOTION OAVIBX is a SIMOTION tool that changes the setpoint variable of an axis so that the moving mechanical system is activated to oscillations as little as possible within the range of its natural frequency.

VULNERABILITY DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

Vulnerability CVE-2025-43715

Nullsoft Scriptable Install System (NSIS) before 3.11 on Windows allows local users to escalate privileges to SYSTEM during an installation, because the temporary plugins directory is created under %WINDIR%\temp and unprivileged users can place a crafted executable file by winning a race condition. This occurs because EW_CREATEDIR does not always set the CreateRestrictedDirectory error flag.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H
CWE	CWE-754: Improper Check for Unusual or Exceptional Conditions

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 (2025-09-09):	Publication Date

TERMS OF USE

The use of Siemens Security Advisories is subject to the terms and conditions listed on: https://www.siemens.com/productcert/terms-of-use.