Smarttech
YOUR 24/7 SECURITY PARTNER

Siemens Security Advisories – 23rd October 2026

Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	185
Authors	Maria-Iasmina Macovei < maria.macovei@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-10-23
Issue Date	2026-10-23

This document and any information therein are confidential property of Smarttech247 and without infringement neither the whole nor any extract may be disclosed, loaned, copied or used for manufacturing, provision of services or other purposes whatsoever without prior written consent of Smarttech247, and no liability is accepted for loss or damage from any cause whatsoever from the use of the document. Smarttech247 retain the right to alter the document at any time unless a written statement to the contrary has been appended.

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released.
Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview

Siemens published multiple security advisories addressing vulnerabilities affecting various industrial products and software components. Successful exploitation of these vulnerabilities could allow attackers to compromise the confidentiality, integrity, and availability of affected systems, potentially leading to unauthorized access, privilege escalation, denial-of-service conditions, exposure of sensitive information, or execution of arbitrary code.

Technical summary

Siemens SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP

CVE-2021-41617
CVSS 3.1 Score: **3.1**

sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

Affected Products

Affected Product and Versions	Remediation
SIMATIC S7-1500 CPU 1518-4 PN/DP MFP (6ES7518-4AX00-1AB0) >= V3.1.7	Currently no fix is available
SIMATIC S7-1500 CPU 1518-4 PN/DP MFP (6ES7518-4AX00-1AC0) >= V3.1.7	Currently no fix is available
SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP (6ES7518-4FX00-1AB0) >= V3.1.7	Currently no fix is available
SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP (6ES7518-4FX00-1AC0) >= V3.1.7	Currently no fix is available

SIPLUS S7-1500 CPU 1518-4 PN/DP MFP (6AG1518-4AX00-4AC0) >= V3.1.7	Currently no fix is available

Mitigations

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

- Limit access to the interactive shell of the additional GNU/Linux subssytem to trusted personnel only.
- Only build and run applications from trusted sources.

Siemens SIMATIC S7-1500 TM MFP

CVE-2023-52927
CVSS 3.1 Score: **7.8**

In the Linux kernel, the following vulnerability has been resolved: netfilter: allow exp not to be removed in nf_ct_find_expectation Currently nf_conntrack_in() calling nf_ct_find_expectation() will remove the exp from the hash table. However, in some scenario, we expect the exp not to be removed when the created ct will not be confirmed, like in OVS and TC conntrack in the following patches. This patch allows exp not to be removed by setting IPS_CONFIRMED in the status of the tmpl.

Affected Products

Affected Product and Versions	Remediation
SIMATIC S7-1500 TM MFP - GNU/Linux subsystem	Currently no fix is available

Mitigations

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

- Limit access to the interactive shell of the additional GNU/Linux subssytem to trusted personnel only.
- Only build and run applications from trusted sources.

Siemens RUGGEDCOM APE1808 Devices

CVE-2026-33387
CVSS 3.1 Score: **4.6**

A template injection vulnerability was discovered in the Dashboards functionality due to improper validation of an input parameter. An authenticated user with the required privileges can define a dashboard containing a malicious payload, or a victim can be socially engineered into importing a malicious dashboard. When the victim views or imports the dashboard, the payload executes in their browser context, allowing the attacker to modify application data or disrupt application availability.

Affected Products

Affected Product and Versions	Remediation
RUGGEDCOM APE1808 with Nozomi Guardian/CMC	Contact customer support to receive patch and update information

CVE-2026-33388
CVSS 3.1 Score: **7.4**

An access control vulnerability was discovered in the Credentials Manager functionality due to insufficient validation of user privileges. A remote authenticated user with limited privileges can view a limited subset of the available entries in the Credentials Manager. The actual credential values are not directly visible, but the user can delete entries or edit their properties. An attacker who deletes or edits an entry can disrupt authentication for dependent devices, and one who manipulates an entry's configuration may be able to indirectly obtain the credentials.

Affected Products

Affected Product and Versions	Remediation
RUGGEDCOM APE1808 with Nozomi Guardian/CMC	Contact customer support to receive patch and update information

CVE-2026-33389
CVSS 3.1 Score: **7.5**

An improper certificate/host key validation vulnerability was discovered in the Smart Polling functionality, which established encrypted connections to target devices without validating the remote host's identity, and no option was provided to enable it. A man-in-the-middle attacker positioned between a sensor and a polled device can, during a polling session, impersonate the device and intercept the communication, including the credentials used to access it. The captured credentials can then be replayed to authenticate against the device itself or against other devices sharing the same credentials, allowing the attacker to access and tamper with the device's data and to disrupt its operations.

Affected Products

Affected Product and Versions	Remediation
RUGGEDCOM APE1808 with Nozomi Guardian/CMC	Contact customer support to receive patch and update information

CVE-2026-33391
CVSS 3.1 Score: **5.4**

An access control vulnerability was discovered in the Smart Polling configuration functionality due to insufficient validation of user privileges. An authenticated user with limited privileges can remotely bypass the intended access control of the web management interface and modify the Smart Polling discovery configuration. This allows the attacker to

disrupt the visibility of assets in the monitored network.

Affected Products

Affected Product and Versions	Remediation
RUGGEDCOM APE1808 with Nozomi Guardian/CMC	Contact customer support to receive patch and update information

CVE-2026-33920
CVSS 3.1 Score: **3.5**

A cross-site request forgery vulnerability was discovered in the login functionality (both standard and SAML) due to missing validation of the anti-CSRF token. An attacker with a valid account can trick a victim into unknowingly authenticating with the attacker's credentials. Any operation performed by the victim in this state is attributed to the attacker's account, compromising the integrity of the audit trail.

Affected Products

Affected Product and Versions	Remediation
RUGGEDCOM APE1808 with Nozomi Guardian/CMC	Contact customer support to receive patch and update information

Siemens Industrial Edge Devices

CVE-2026-44414
CVSS 3.1 Score: **6.8**

Affected systems do not properly restrict access to internal APIs and paths for authenticated users. This could allow an authenticated remote attacker to access sensitive internal information, which in the worst case could be leveraged to facilitate unauthorized access to the system.

CVE-2026-44415
CVSS 3.1 Score: **9.1**

Affected systems do not properly restrict access to internal APIs and paths for authenticated users. This could allow an authenticated remote attacker to access sensitive internal information, which in the worst case could be leveraged to facilitate unauthorized access to the system or result in the deletion of data.

Affected Products

Affected Product and Versions	Remediation
Industrial Edge Cloud Device (IECD) < V1.28.1	Update to V1.28.1 or later version
Industrial Edge Own Device (IEOD) < V1.28.1	Update to V1.28.1 or later version
Industrial Edge Virtual Device (IEVD) < V1.28.1	Update to V1.28.1 or later version

SCALANCE LPE9413 (6GK5998-3GS01-2AC2)	Currently no fix is planned
SCALANCE LPE9433 (6GK5998-3GS11-2AC2)	Currently no fix is available
SIMATIC IoT2050 Advanced IED (6ES7647-0BW00-1YA2) < V1.28.1-2	Update to V1.28.1-2 or later version
SIMATIC IoT2050 SM IED (6ES7647-0CW00-1AA2) < V1.28.1-2	Update to V1.28.1-2 or later version
SIMATIC IPC BX-21A Industrial Edge Device < V1.28.1-2	Update to V1.28.1-2 or later version
SIMATIC IPC BX-39A Industrial Edge Device < V3.2.0-17	Update to V3.2.0-17 or later version
SIMATIC IPC BX-59A Industrial Edge Device < V3.2.0-17	Update to V3.2.0-17 or later version
SIMATIC IPC127E Industrial Edge Device < V3.2.0-17	Update to V3.2.0-17 or later version
SIMATIC IPC227E Industrial Edge Device < V3.2.0-17	Update to V3.2.0-17 or later version
SIMATIC IPC227G Industrial Edge Device < V3.2.0-17	Update to V3.2.0-17 or later version
SIMATIC IPC427E Industrial Edge Device < V3.2.0-17	Update to V3.2.0-17 or later version
SIMATIC IPC847E Industrial Edge Device < V3.2.0-17	Update to V3.2.0-17 or later version
Industrial Edge Cloud Device (IECD) < V1.28.1	Currently no fix is planned
Industrial Edge Own Device (IEOD) < V1.28.1	Currently no fix is planned
Industrial Edge Virtual Device (IEVD) < V1.28.1	Currently no fix is planned
SCALANCE LPE9413 (6GK5998-3GS01-2AC2)	Currently no fix is planned
SCALANCE LPE9433 (6GK5998-3GS11-2AC2)	Currently no fix is planned
SIMATIC IoT2050 Advanced IED (6ES7647-0BW00-1YA2) < V1.28.1-2	Currently no fix is planned
SIMATIC IoT2050 SM IED (6ES7647-0CW00-1AA2) < V1.28.1-2	Currently no fix is planned
SIMATIC IPC BX-21A Industrial Edge Device < V1.28.1-2	Currently no fix is planned
SIMATIC IPC BX-39A Industrial Edge Device < V3.2.0-17	Currently no fix is planned

SIMATIC IPC BX-59A Industrial Edge Device < V3.2.0-17	Currently no fix is planned
SIMATIC IPC127E Industrial Edge Device < V3.2.0-17	Currently no fix is planned
SIMATIC IPC227E Industrial Edge Device < V3.2.0-17	Currently no fix is planned
SIMATIC IPC227G Industrial Edge Device < V3.2.0-17	Currently no fix is planned
SIMATIC IPC427E Industrial Edge Device < V3.2.0-17	Currently no fix is planned
SIMATIC IPC847E Industrial Edge Device < V3.2.0-17	Currently no fix is planned
SIMATIC HMI MTP1200 Comfort Pro for stand (expandable, flange at the bottom) (6AV2128-3MB27-1BX0)	Currently no fix is planned
SIMATIC HMI MTP1200 Comfort Pro for support arm (expandable, round tube) and extension unit (6AV2128-3MB27-0BX0)	Currently no fix is planned
SIMATIC HMI MTP1200 Comfort Pro for support arm (not extendable, flange on top) (6AV2128-3MB27-0AX0)	Currently no fix is planned
SIMATIC HMI MTP1200 Comfort Pro neutral design for stand (expandable, flange at the bottom) (6AV2128-3MB57-1BX0)	Currently no fix is planned
SIMATIC HMI MTP1200 Comfort Pro neutral design for support arm (expandable, round tube) and extension (6AV2128-3MB57-0BX0)	Currently no fix is planned
SIMATIC HMI MTP1200 Comfort Pro neutral design for support arm (not extendable, flange on top) (6AV2128-3MB57-0AX0)	Currently no fix is planned
SIMATIC HMI MTP1200 Unified Comfort Panel (6AV2128-3MB06-0AX1)	Currently no fix is planned
SIMATIC HMI MTP1200 Unified Comfort Panel hygienic (6AV2128-3MB40-0AX0)	Currently no fix is planned
SIMATIC HMI MTP1200 Unified Comfort Panel hygienic neutral design (6AV2128-3MB70-0AX0)	Currently no fix is planned
SIMATIC HMI MTP1200 Unified Comfort Panel neutral design (6AV2128-3MB36-0AX1)	Currently no fix is planned

SIMATIC HMI MTP1500 Comfort Pro for stand (expandable, flange at the bottom) (6AV2128-3QB27-1BX0)	Currently no fix is planned
SIMATIC HMI MTP1500 Comfort Pro for support arm (expandable, round tube) and extension unit (6AV2128-3QB27-0BX0)	Currently no fix is planned
SIMATIC HMI MTP1500 Comfort Pro for support arm (not extendable, flange on top) (6AV2128-3QB27-0AX0)	Currently no fix is planned
SIMATIC HMI MTP1500 Comfort Pro neutral design for stand (expandable, flange at the bottom) (6AV2128-3QB57-1BX0)	Currently no fix is planned
SIMATIC HMI MTP1500 Comfort Pro neutral design for support arm (expandable, round tube) and extension (6AV2128-3QB57-0BX0)	Currently no fix is planned
SIMATIC HMI MTP1500 Comfort Pro neutral design for support arm (not extendable, flange on top) (6AV2128-3QB57-0AX0)	Currently no fix is planned
SIMATIC HMI MTP1500 Unified Comfort Panel (6AV2128-3QB06-0AX1)	Currently no fix is planned
SIMATIC HMI MTP1500 Unified Comfort Panel hygienic (6AV2128-3QB40-0AX0)	Currently no fix is planned
SIMATIC HMI MTP1500 Unified Comfort Panel hygienic neutral design (6AV2128-3QB70-0AX0)	Currently no fix is planned
SIMATIC HMI MTP1500 Unified Comfort Panel neutral design (6AV2128-3QB36-0AX1)	Currently no fix is planned
SIMATIC HMI MTP1900 Comfort Pro for stand (expandable, flange at the bottom) (6AV2128-3UB27-1BX0)	Currently no fix is planned
SIMATIC HMI MTP1900 Comfort Pro for support arm (expandable, round tube) and extension unit (6AV2128-3UB27-0BX0)	Currently no fix is planned
SIMATIC HMI MTP1900 Comfort Pro for support arm (not extendable, flange on top) (6AV2128-3UB27-0AX0)	Currently no fix is planned
SIMATIC HMI MTP1900 Comfort Pro neutral design for stand (expandable, flange at the bottom) (6AV2128-3UB57-1BX0)	Currently no fix is planned
SIMATIC HMI MTP1900 Comfort Pro neutral design for support arm (expandable, round tube) and extension (6AV2128-3UB57-0BX0)	Currently no fix is planned

SIMATIC HMI MTP1900 Comfort Pro neutral design for support arm (not extendable, flange on top) (6AV2128-3UB57-0AX0)	Currently no fix is planned
SIMATIC HMI MTP1900 Unified Comfort Panel (6AV2128-3UB06-0AX1)	Currently no fix is planned
SIMATIC HMI MTP1900 Unified Comfort Panel hygienic (6AV2128-3UB40-0AX0)	Currently no fix is planned
SIMATIC HMI MTP1900 Unified Comfort Panel hygienic neutral design (6AV2128-3UB70-0AX0)	Currently no fix is planned
SIMATIC HMI MTP1900 Unified Comfort Panel neutral design (6AV2128-3UB36-0AX1)	Currently no fix is planned
SIMATIC HMI MTP2200 Comfort Pro for stand (expandable, flange at the bottom) (6AV2128-3XB27-1BX0)	Currently no fix is planned
SIMATIC HMI MTP2200 Comfort Pro for support arm (expandable, round tube) and extension unit (6AV2128-3XB27-0BX0)	Currently no fix is planned
SIMATIC HMI MTP2200 Comfort Pro for support arm (not extendable, flange on top) (6AV2128-3XB27-0AX0)	Currently no fix is planned
SIMATIC HMI MTP2200 Comfort Pro neutral design for stand (expandable, flange at the bottom) (6AV2128-3XB57-1BX0)	Currently no fix is planned
SIMATIC HMI MTP2200 Comfort Pro neutral design for support arm (expandable, round tube) and extension (6AV2128-3XB57-0BX0)	Currently no fix is planned
SIMATIC HMI MTP2200 Comfort Pro neutral design for support arm (not extendable, flange on top) (6AV2128-3XB57-0AX0)	Currently no fix is planned
SIMATIC HMI MTP2200 Unified Comfort Hygienic (6AV2128-3XB40-0AX0)	Currently no fix is planned
SIMATIC HMI MTP2200 Unified Comfort Hygienic neutral design (6AV2128-3XB70-0AX0)	Currently no fix is planned
SIMATIC HMI MTP2200 Unified Comfort Panel (6AV2128-3XB06-0AX1)	Currently no fix is planned
SIMATIC HMI MTP2200 Unified Comfort Panel neutral design (6AV2128-3XB36-0AX1)	Currently no fix is planned
SIMATIC HMI MTP700 Unified Comfort Panel (6AV2128-3GB06-0AX1)	Currently no fix is planned

SIMATIC HMI MTP700 Unified Comfort Panel hygienic neutral design (6AV2128-3GB40-0AX0)	Currently no fix is planned
SIMATIC HMI MTP700 Unified Comfort Panel hygienic neutral design (6AV2128-3GB70-0AX0)	Currently no fix is planned
SIMATIC HMI MTP700, Unified Comfort Panel neutral design (6AV2128-3GB36-0AX1)	Currently no fix is planned
SIMATIC HMI MTP1000 Unified Comfort Panel (6AV2128-3KB06-0AX1)	Currently no fix is planned
SIPLUS HMI MTP1000 Unified Comfort (6AG1128-3KB06-4AX1)	Currently no fix is planned
SIPLUS HMI MTP1200 Unified Comfort (6AG1128-3MB06-4AX1)	Currently no fix is planned
SIPLUS HMI MTP700 Unified Comfort (6AG1128-3GB06-4AX1)	Currently no fix is planned
SIMATIC HMI MTP1000 Unified Comfort Panel hygienic (6AV2128-3KB40-0AX0)	Currently no fix is planned
SIMATIC HMI MTP1000 Unified Comfort Panel hygienic neutral design (6AV2128-3KB70-0AX0)	Currently no fix is planned
SIMATIC HMI MTP1000, Unified Comfort Panel neutral (6AV2128-3KB36-0AX1)	

Siemens RUGGEDCOM CROSSBOW Station Access Controller

CVE-2025-6965
CVSS 3.1 Score: **7.7**

There exists a vulnerability in SQLite versions before 3.50.2 where the number of aggregate terms could exceed the number of columns available. This could lead to a memory corruption issue. We recommend upgrading to version 3.50.2 or above.

CVE-2025-70873
CVSS 3.1 Score: **7.5**

An information disclosure issue in the zipfileInflate function in the zipfile extension in SQLite v3.51.1 and earlier allows attackers to obtain heap memory via supplying a crafted ZIP file.

CVE-2025-71316
CVSS 3.1 Score: **9.8**

SQLite 'sqldiff.exe' does not securely handle the way the Microsoft Windows C runtime

converts Unicode characters to ANSI codepages. An attacker could use the '-L' option to load an arbitrary DLL with a crafted command line argument string that results in command line file arguments being misinterpreted as command line options. Fixed on or around 2025-12-26.

CVE-2026-11822
CVSS 3.1 Score: **7.8**

SQLite before 3.53.2 contains memory corruption vulnerabilities in the FTS5 full-text search extension that allow attackers to cause process crashes, memory exhaustion, or arbitrary code execution by supplying a crafted database with malformed FTS5 page data. Attackers can trigger an out-of-bounds read in fts5LeafSeek() via an attacker-controlled loop bound and a heap buffer overflow write in fts5ChunkIterate() through a crafted continuation page causing an integer underflow, exploitable when an FTS5 MATCH query is executed against the malicious database.

CVE-2026-11824
CVSS 3.1 Score: **7.8**

SQLite before 3.53.2 contains a heap-based buffer overflow vulnerability in the FTS5 full-text search extension that allows attackers to cause a crash or execute arbitrary code by supplying a crafted database with malicious continuation page metadata specifying a szLeaf value smaller than 4. Attackers can trigger an integer underflow in fts5ChunkIterate() causing an inflated remaining byte count during FTS5 MATCH query processing, leading to a heap buffer overflow of attacker-controlled data in applications compiled with SQLITE_ENABLE_FTS5.

Affected Products

Affected Product and Versions	Remediation
RUGGEDCOM CROSSBOW Station Access Controller (SAC) < V6.0	Update to V6.0 or later version

Siemens SIMATIC S7 PLCs Web Server

CVE-2026-63350
CVSS 3.1 Score: **9.6**

Affected devices do not properly restrict executable content contained in imported trace files. This could allow an attacker to social engineer an authorized user who holds the function right “Read diagnostics” into importing a specially crafted trace file. Successful exploitation could allow attacker-controlled JavaScript to execute in the user’s browser session and perform PLC operations through the web server within the scope of the user’s authorization.

CVE-2026-63351
CVSS 3.1 Score: **6.1**

Affected devices do not properly validate and sanitize visual properties of calculated signals contained in imported CSV trace files before rendering them on the Trace page. This could

allow an attacker to social engineer an authorized user who holds the function right “Read diagnostics” into importing a specially crafted trace file. Successful exploitation could allow attacker-controlled JavaScript to execute in the user’s browser session and perform PLC operations through the web server within the scope of the user’s authorization.

CVE-2026-63352
CVSS 3.1 Score: **6.1**

Affected devices do not properly sanitize calculated signal data contained in imported CSV trace files before rendering it on the Trace page. This could allow an attacker to social engineer an authorized user who holds the function right “Read diagnostics” into importing a specially crafted trace file. Successful exploitation could allow attacker-controlled JavaScript to execute in the user’s browser session and perform PLC operations through the web server within the scope of the user’s authorization.

CVE-2026-63353
CVSS 3.1 Score: **9.6**

Affected devices do not properly sanitize comment fields contained in imported trace files before rendering them on the Trace page. This could allow an attacker to social engineer an authorized user who holds the function right “Read diagnostics” into importing a specially crafted trace file. Successful exploitation could allow attacker-controlled JavaScript to execute in the user’s browser session and perform PLC operations through the web server within the scope of the user’s authorization.

CVE-2026-63354
CVSS 3.1 Score: **9.6**

Affected devices do not properly validate and sanitize visual marker data contained in imported CSV trace files before rendering it on the Trace page. This could allow an attacker to social engineer an authorized user who holds the function right “Read diagnostics” into importing a specially crafted trace file. Successful exploitation could allow attacker-controlled JavaScript to execute in the user’s browser session and perform PLC operations through the web server within the scope of the user’s authorization.

CVE-2026-63355
CVSS 3.1 Score: **6.1**

Affected devices do not properly sanitize signal names contained in imported CSV trace files before rendering them in selection menus on the Trace page. This could allow an attacker to social engineer an authorized user who holds the function right “Read diagnostics” into importing a specially crafted trace file. Attacker-controlled JavaScript could be executed in the user’s browser session when the user subsequently interacts with an affected selection menu.

CVE-2026-63356
CVSS 3.1 Score: **6.1**

Affected devices do not properly sanitize calculated signal names contained in imported CSV trace files before including them in error messages on the Trace page. This could allow an attacker to social engineer an authorized user who holds the function right “Read

diagnostics" into importing a specially crafted trace file. Attacker-controlled JavaScript could be executed in the user's browser session when the resulting error message is displayed.

CVE-2026-63357
CVSS 3.1 Score: **6.1**

Affected devices do not properly sanitize calculated signal data contained in imported calculated signal files before rendering it on the Trace page. This could allow an attacker to social engineer an authorized user who holds the function right "Read diagnostics" into importing a specially crafted file. Successful exploitation could allow attacker-controlled JavaScript to execute in the user's browser session and perform PLC operations through the web server within the scope of the user's authorization.

Affected Products

The following versions of **Siemens SIMATIC S7 PLCs Web Server** are affected:

- SIMATIC Drive Controller CPU 1504D TF (6ES7615-4DF10-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC Drive Controller CPU 1507D TF (6ES7615-7DF10-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC ET 200SP CPU 1510SP F-1 PN (6ES7510-1SJ01-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC ET 200SP CPU 1510SP F-1 PN (6ES7510-1SK03-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC ET 200SP CPU 1510SP-1 PN (6ES7510-1DJ01-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC ET 200SP CPU 1510SP-1 PN (6ES7510-1DK03-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC ET 200SP CPU 1512SP F-1 PN (6ES7512-1SK01-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC ET 200SP CPU 1512SP F-1 PN (6ES7512-1SM03-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC ET 200SP CPU 1512SP-1 PN (6ES7512-1DK01-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC ET 200SP CPU 1512SP-1 PN (6ES7512-1DM03-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC ET 200SP CPU 1514SP F-2 PN (6ES7514-2SN03-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC ET 200SP CPU 1514SP-2 PN (6ES7514-2DN03-0AB0) vers:all/* (CVE-

2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)

- SIMATIC ET 200SP CPU 1514SPT F-2 PN (6ES7514-2WN03-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC ET 200SP CPU 1514SPT-2 PN (6ES7514-2VN03-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) V2 CPUs - Windows OS vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) V3 CPUs - Industrial OS vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) V3 CPUs - Windows OS vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC ET 200SP Open Controller CPU 1515SP PC3 V4 CPUs vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1511-1 PN (6ES7511-1AK00-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1511-1 PN (6ES7511-1AK01-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1511-1 PN (6ES7511-1AK02-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1511-1 PN (6ES7511-1AL03-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1511C-1 PN (6ES7511-1CK00-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1511C-1 PN (6ES7511-1CK01-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1511C-1 PN (6ES7511-1CL03-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1511F-1 PN (6ES7511-1FK01-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1511F-1 PN (6ES7511-1FK02-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354,

CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1511F-1 PN (6ES7511-1FL03-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1511T-1 PN (6ES7511-1TK01-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1511T-1 PN (6ES7511-1TL03-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1511TF-1 PN (6ES7511-1UK01-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1511TF-1 PN (6ES7511-1UL03-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1512C-1 PN (6ES7512-1CK00-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1512C-1 PN (6ES7512-1CK01-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1512C-1 PN (6ES7512-1CM03-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1513-1 PN (6ES7513-1AL01-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1513-1 PN (6ES7513-1AL02-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1513-1 PN (6ES7513-1AM03-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1513F-1 PN (6ES7513-1FL01-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1513F-1 PN (6ES7513-1FL02-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1513F-1 PN (6ES7513-1FM03-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1513pro F-2 PN (6ES7513-2GM03-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1513pro-2 PN (6ES7513-2PM03-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1515-2 PN (6ES7515-2AM01-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)

- SIMATIC S7-1500 CPU 1515-2 PN (6ES7515-2AM02-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1515-2 PN (6ES7515-2AN03-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1515F-2 PN (6ES7515-2FM01-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1515F-2 PN (6ES7515-2FM02-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1515F-2 PN (6ES7515-2FN03-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1515T-2 PN (6ES7515-2TM01-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1515T-2 PN (6ES7515-2TN03-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1515TF-2 PN (6ES7515-2UM01-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1515TF-2 PN (6ES7515-2UN03-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1516-3 PN/DP (6ES7516-3AN01-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1516-3 PN/DP (6ES7516-3AN02-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1516-3 PN/DP (6ES7516-3AP03-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1516F-3 PN/DP (6ES7516-3FN01-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1516F-3 PN/DP (6ES7516-3FN02-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1516F-3 PN/DP (6ES7516-3FP03-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1516pro F-2 PN (6ES7516-2GP03-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1516pro-2 PN (6ES7516-2PP03-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1516T-3 PN (6ES7516-3TP10-0AB0) vers:all/* (CVE-2026-

63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)

- SIMATIC S7-1500 CPU 1516T-3 PN/DP (6ES7516-3TN00-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1516TF-3 PN (6ES7516-3UP10-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1516TF-3 PN/DP (6ES7516-3UN00-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1517-3 PN (6ES7517-3AQ10-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1517-3 PN/DP (6ES7517-3AP00-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1517F-3 PN (6ES7517-3FQ10-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1517F-3 PN/DP (6ES7517-3FP00-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1517F-3 PN/DP (6ES7517-3FP01-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1517T-3 PN (6ES7517-3TQ10-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1517T-3 PN/DP (6ES7517-3TP00-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1517TF-3 PN (6ES7517-3UQ10-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1517TF-3 PN/DP (6ES7517-3UP00-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1518-3 PN (6ES7518-3AT10-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1518-4 PN/DP (6ES7518-4AP00-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1518-4 PN/DP MFP (6ES7518-4AX00-1AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1518-4 PN/DP MFP (6ES7518-4AX00-1AC0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1518F-3 PN (6ES7518-3FT10-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354,

CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)

- SIMATIC S7-1500 CPU 1518F-4 PN/DP (6ES7518-4FP00-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP (6ES7518-4FX00-1AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP (6ES7518-4FX00-1AC0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1518T-3 PN (6ES7518-3TT10-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1518T-4 PN/DP (6ES7518-4TP00-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1518TF-3 PN (6ES7518-3UT10-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU 1518TF-4 PN/DP (6ES7518-4UP00-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU S7-1518-4 PN/DP ODK (6ES7518-4AP00-3AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 CPU S7-1518F-4 PN/DP ODK (6ES7518-4FP00-3AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 ET 200pro: CPU 1513PRO F-2 PN (6ES7513-2GL00-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 ET 200pro: CPU 1513PRO-2 PN (6ES7513-2PL00-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 ET 200pro: CPU 1516PRO F-2 PN (6ES7516-2GN00-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 ET 200pro: CPU 1516PRO-2 PN (6ES7516-2PN00-0AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 Software Controller CPU 1507S F V2 vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 Software Controller CPU 1507S F V3 vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 Software Controller CPU 1507S F V4 vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 Software Controller CPU 1507S V2 vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)

- SIMATIC S7-1500 Software Controller CPU 1507S V3 vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 Software Controller CPU 1507S V4 vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 Software Controller CPU 1508S F V2 vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 Software Controller CPU 1508S F V3 vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 Software Controller CPU 1508S F V4 vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 Software Controller CPU 1508S T V3 vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 Software Controller CPU 1508S TF V3 vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 Software Controller CPU 1508S V2 vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 Software Controller CPU 1508S V3 vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 Software Controller CPU 1508S V4 vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 Software Controller Linux V2 vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-1500 Software Controller Linux V3 vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIMATIC S7-PLCSIM Advanced vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS ET 200SP CPU 1510SP F-1 PN (6AG1510-1SJ01-2AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS ET 200SP CPU 1510SP F-1 PN RAIL (6AG2510-1SJ01-1AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS ET 200SP CPU 1510SP-1 PN (6AG1510-1DJ01-2AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS ET 200SP CPU 1510SP-1 PN (6AG1510-1DJ01-7AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS ET 200SP CPU 1510SP-1 PN RAIL (6AG2510-1DJ01-1AB0) vers:all/* (CVE-

2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)

- SIPLUS ET 200SP CPU 1510SP-1 PN RAIL (6AG2510-1DJ01-4AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS ET 200SP CPU 1512SP F-1 PN (6AG1512-1SK01-2AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS ET 200SP CPU 1512SP F-1 PN (6AG1512-1SK01-7AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS ET 200SP CPU 1512SP F-1 PN RAIL (6AG2512-1SK01-1AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS ET 200SP CPU 1512SP F-1 PN RAIL (6AG2512-1SK01-4AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS ET 200SP CPU 1512SP-1 PN (6AG1512-1DK01-2AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS ET 200SP CPU 1512SP-1 PN (6AG1512-1DK01-7AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS ET 200SP CPU 1512SP-1 PN RAIL (6AG2512-1DK01-1AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS ET 200SP CPU 1512SP-1 PN RAIL (6AG2512-1DK01-4AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS S7-1500 CPU 1511-1 PN (6AG1511-1AK01-2AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS S7-1500 CPU 1511-1 PN (6AG1511-1AK01-7AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS S7-1500 CPU 1511-1 PN (6AG1511-1AK02-2AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS S7-1500 CPU 1511-1 PN (6AG1511-1AK02-7AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS S7-1500 CPU 1511-1 PN T1 RAIL (6AG2511-1AK01-1AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS S7-1500 CPU 1511-1 PN T1 RAIL (6AG2511-1AK02-1AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS S7-1500 CPU 1511-1 PN TX RAIL (6AG2511-1AK01-4AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS S7-1500 CPU 1511-1 PN TX RAIL (6AG2511-1AK02-4AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-

63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)

- SIPLUS S7-1500 CPU 1511F-1 PN (6AG1511-1FK01-2AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS S7-1500 CPU 1511F-1 PN (6AG1511-1FK02-2AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS S7-1500 CPU 1513-1 PN (6AG1513-1AL01-2AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS S7-1500 CPU 1513-1 PN (6AG1513-1AL01-7AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS S7-1500 CPU 1513-1 PN (6AG1513-1AL02-2AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS S7-1500 CPU 1513-1 PN (6AG1513-1AL02-7AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS S7-1500 CPU 1513F-1 PN (6AG1513-1FL01-2AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS S7-1500 CPU 1513F-1 PN (6AG1513-1FL02-2AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS S7-1500 CPU 1515F-2 PN (6AG1515-2FM01-2AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS S7-1500 CPU 1515F-2 PN (6AG1515-2FM02-2AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS S7-1500 CPU 1515F-2 PN RAIL (6AG2515-2FM02-4AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS S7-1500 CPU 1515F-2 PN T2 RAIL (6AG2515-2FM01-2AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN01-2AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN01-7AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN02-2AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN02-7AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS S7-1500 CPU 1516-3 PN/DP RAIL (6AG2516-3AN02-4AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)

- SIPLUS S7-1500 CPU 1516-3 PN/DP TX RAIL (6AG2516-3AN01-4AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS S7-1500 CPU 1516F-3 PN/DP (6AG1516-3FN01-2AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS S7-1500 CPU 1516F-3 PN/DP (6AG1516-3FN02-2AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS S7-1500 CPU 1516F-3 PN/DP RAIL (6AG2516-3FN02-2AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS S7-1500 CPU 1516F-3 PN/DP RAIL (6AG2516-3FN02-4AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS S7-1500 CPU 1518-4 PN/DP (6AG1518-4AP00-4AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS S7-1500 CPU 1518-4 PN/DP MFP (6AG1518-4AX00-4AC0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)
- SIPLUS S7-1500 CPU 1518F-4 PN/DP (6AG1518-4FP00-4AB0) vers:all/* (CVE-2026-63350, CVE-2026-63351, CVE-2026-63352, CVE-2026-63353, CVE-2026-63354, CVE-2026-63355, CVE-2026-63356, CVE-2026-63357)

Siemens WinCC

CVE-2026-59241
CVSS 3.1 Score: **8.8**

The affected application does not sufficiently restrict the permissions assigned to a database role. This could allow an authenticated remote attacker with database access to escalate privileges and execute arbitrary commands on the host system where SIMATIC WinCC is installed, potentially leading to a compromise of the system.

Affected Products

Affected Product and Versions	Remediation
SIMATIC WinCC V7.5	Currently no fix is available
SIMATIC WinCC V8.0 < V8.0 Update 11	Update to V8.0 Update 11 or later version
SIMATIC WinCC V8.1 < V8.1 Update 7	Update to V8.1 Update 7 or later version

Siemens RUGGEDCOM CROSSBOW

CVE-2026-89196
CVSS 3.1 Score: **8.8**

Affected devices do not properly validate or sanitize input in facility names processed during the Bulk Import/Export workflow. This could allow an authenticated attacker with specific

privileges to execute arbitrary SQL commands on the underlying database.

CVE-2026-89197
CVSS 3.1 Score: **8.8**

Affected devices do not properly validate or sanitize input in the Value field of notification conditions processed during the Notification Profile configuration. This could allow an authenticated attacker with specific privileges to execute arbitrary SQL commands on the underlying database.

CVE-2026-89198
CVSS 3.1 Score: **8.8**

Affected devices do not properly validate or sanitize the filename of firmware files uploaded to the system. This could allow an authenticated attacker with specific privileges to execute arbitrary SQL commands on the underlying database.

CVE-2026-89199
CVSS 3.1 Score: **8.8**

Affected devices do not properly restrict access to sensitive configuration items via specific database queries. This could allow an authenticated attacker to retrieve administrative credentials for various internal systems, leading to unauthorized information disclosure and privilege escalation.

CVE-2026-89200
CVSS 3.1 Score: **6.7**

Affected devices do not properly validate or sanitize input in the Name and Value fields for custom file labels. This could allow an authenticated attacker with administrative privileges to execute arbitrary SQL commands on the underlying database.

CVE-2026-89201
CVSS 3.1 Score: **7.5**

Affected devices do not properly validate or sanitize input in device group or facility names processed during the Bulk Export workflow. This could allow an authenticated attacker with specific privileges to execute arbitrary SQL commands on the underlying database.

CVE-2026-89202
CVSS 3.1 Score: **6.5**

Affected devices do not properly perform authorization checks for device disconnection requests. This could allow an authenticated attacker with minimal privileges to disconnect active sessions of other users, including administrators, leading to a denial of service.

CVE-2026-89203
CVSS 3.1 Score: **4.3**

Affected devices do not properly restrict access to various database queries, allowing users to retrieve system-wide information that is not intended for their privilege level. This could allow an authenticated attacker to gather sensitive information about the system's

infrastructure, including details on all devices, substations, users, and scheduled activities.

CVE-2026-89204
CVSS 3.1 Score: **5.4**

Affected devices do not properly restrict access to database queries used for subnet management. This could allow an authenticated attacker to read, modify, or delete subnet configurations, leading to unauthorized information disclosure and data manipulation.

CVE-2026-89205
CVSS 3.1 Score: **6.3**

Affected devices do not properly perform server-side authorization checks for requests to schedule special operations. This could allow an authenticated attacker with minimal privileges to schedule unauthorized operations on devices.

CVE-2026-89206
CVSS 3.1 Score: **6.3**

Affected devices do not properly perform server-side authorization checks for requests to modify the state of scheduled actions. This could allow an authenticated attacker with minimal privileges to retry, stop, or delete scheduled tasks without proper authorization.

Affected Products

Affected Product and Versions	Remediation
RUGGEDCOM CROSSBOW < V6.0	Update to V6.0 or later version

Siemens SIMATIC S7 Webserver API

CVE-2026-85114
CVSS 3.1 Score: **7.5**

Affected applications do not properly validate filenames received from remote servers during ticket downloads. This could allow an attacker who can manipulate the ticket response to write arbitrary files outside the intended download directory and, when overwriting is enabled, replace existing files accessible to the application.

CVE-2026-85115
CVSS 3.1 Score: **5.5**

Affected applications do not properly redact PLC restore passwords from HTTP error exception messages. This could allow an attacker with access to logs or other diagnostic output to obtain the plaintext restore password and potentially perform unauthorized operations on the PLC.

Affected Products

Affected Product and Versions	Remediation
.NET Client Library for SIMATIC S7 Webserver API < V3.3.61	Update to V3.3.61 or later version

.NET Client Library for SIMATIC S7 Webserver API < V3.3.62	Update to V3.3.62 or later version

Siemens Industrial Edge Device Kit

CVE-2026-44414
CVSS 3.1 Score: **6.8**

Affected systems do not properly restrict access to internal APIs and paths for authenticated users. This could allow an authenticated remote attacker to access sensitive internal information, which in the worst case could be leveraged to facilitate unauthorized access to the system.

CVE-2026-44415
CVSS 3.1 Score: **9.1**

Affected systems do not properly restrict access to internal APIs and paths for authenticated users. This could allow an authenticated remote attacker to access sensitive internal information, which in the worst case could be leveraged to facilitate unauthorized access to the system or result in the deletion of data.

Affected Products

The following versions of Siemens Industrial Edge Device Kit are affected:

- Industrial Edge Device Kit - arm64 V1.10 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - arm64 V1.11 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - arm64 V1.12 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - arm64 V1.13 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - arm64 V1.14 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - arm64 V1.15 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - arm64 V1.16 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - arm64 V1.17 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - arm64 V1.18 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - arm64 V1.19 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - arm64 V1.20 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - arm64 V1.21 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - arm64 V1.22 vers:all/* (CVE-2026-44414, CVE-2026-44415)

- Industrial Edge Device Kit - arm64 V1.23 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - arm64 V1.24 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - arm64 V1.25 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - arm64 V1.26 vers:intdot/<1.26.2.1 (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - arm64 V1.27 vers:intdot/<1.27.1.1 (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - arm64 V1.28 vers:intdot/<1.28.0.6 (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - arm64 V1.5 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - arm64 V1.6 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - arm64 V1.7 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - arm64 V1.8 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - arm64 V1.9 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - x86-64 V1.10 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - x86-64 V1.11 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - x86-64 V1.12 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - x86-64 V1.13 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - x86-64 V1.14 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - x86-64 V1.15 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - x86-64 V1.16 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - x86-64 V1.17 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - x86-64 V1.18 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - x86-64 V1.19 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - x86-64 V1.20 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - x86-64 V1.21 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - x86-64 V1.22 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - x86-64 V1.23 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - x86-64 V1.24 vers:all/* (CVE-2026-44414, CVE-2026-44415)

- Industrial Edge Device Kit - x86-64 V1.25 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - x86-64 V1.26 vers:intdot/<1.26.2.1 (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - x86-64 V1.27 vers:intdot/<1.27.1.1 (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - x86-64 V1.28 vers:intdot/<1.28.0.6 (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - x86-64 V1.5 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - x86-64 V1.6 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - x86-64 V1.7 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - x86-64 V1.8 vers:all/* (CVE-2026-44414, CVE-2026-44415)
- Industrial Edge Device Kit - x86-64 V1.9 vers:all/* (CVE-2026-44414, CVE-2026-44415)

Siemens APOGEE, TALON and Desigo PXC/PXM Products

CVE-2026-89208
CVSS 3.1 Score: **5.3**

The affected product does not properly validate input bounds before accessing packet data. This could allow an unauthenticated remote attacker to trigger memory reads outside the intended packet boundaries.

CVE-2026-102073
CVSS 3.1 Score: **8.2**

The affected product web service does not properly validate the length of user-controllable input. This could allow an unauthenticated remote attacker to read portions of device memory or to cause a denial-of-service condition.

CVE-2026-102074
CVSS 3.1 Score: **7.5**

The affected product FTP service does not properly validate the length of user-controllable input. This could allow an unauthenticated remote attacker to cause a denial of service.

CVE-2026-102075
CVSS 3.1 Score: **7.5**

The affected product web service does not properly validate user input in multipart handling. This could allow an unauthenticated remote attacker to cause a denial of service.

CVE-2026-102076
CVSS 3.1 Score: **7.5**

The affected product web service does not properly validate user-supplied input in upload code. This could allow an unauthenticated remote attacker to cause a denial of service.

Affected Products

The following versions of Siemens APOGEE, TALON and Desigo PXC/PXM Products are affected:

- APOGEE MBC (PPC) (BACnet) vers:all/* (CVE-2026-102073, CVE-2026-102074, CVE-2026-102075, CVE-2026-102076)
- APOGEE MBC (PPC) (P2 Ethernet) vers:all/* (CVE-2026-102073, CVE-2026-102074, CVE-2026-102075, CVE-2026-102076)
- APOGEE MEC (PPC) (BACnet) vers:all/* (CVE-2026-102073, CVE-2026-102074, CVE-2026-102075, CVE-2026-102076)
- APOGEE MEC (PPC) (P2 Ethernet) vers:all/* (CVE-2026-102073, CVE-2026-102074, CVE-2026-102075, CVE-2026-102076)
- APOGEE PXC Compact (BACnet) vers:intdot/<3.5.7 (CVE-2026-102073, CVE-2026-102074, CVE-2026-102075, CVE-2026-102076)
- APOGEE PXC Compact (P2 Ethernet) vers:intdot/<2.8.21 (CVE-2026-102073, CVE-2026-102074, CVE-2026-102075, CVE-2026-102076)
- APOGEE PXC Modular (BACnet) vers:intdot/<3.5.7 (CVE-2026-102073, CVE-2026-102074, CVE-2026-102075, CVE-2026-102076)
- APOGEE PXC Modular (P2 Ethernet) vers:intdot/<2.8.21 (CVE-2026-102073, CVE-2026-102074, CVE-2026-102075, CVE-2026-102076)
- Desigo PXC00-E.D vers:intdot/>=2.3 (CVE-2026-89208)
- Desigo PXC00-U vers:intdot/>=2.3 (CVE-2026-89208)
- Desigo PXC001-E.D vers:intdot/>=2.3 (CVE-2026-89208)
- Desigo PXC100-E.D vers:intdot/>=2.3 (CVE-2026-89208)
- Desigo PXC12-E.D vers:intdot/>=2.3 (CVE-2026-89208)
- Desigo PXC128-U vers:intdot/>=2.3 (CVE-2026-89208)
- Desigo PXC200-E.D vers:intdot/>=2.3 (CVE-2026-89208)
- Desigo PXC22-E.D vers:intdot/>=2.3 (CVE-2026-89208)
- Desigo PXC22.1-E.D vers:intdot/>=2.3 (CVE-2026-89208)
- Desigo PXC36.1-E.D vers:intdot/>=2.3 (CVE-2026-89208)
- Desigo PXC50-E.D vers:intdot/>=2.3 (CVE-2026-89208)
- Desigo PXC64-U vers:intdot/>=2.3 (CVE-2026-89208)
- Desigo PXM20-E vers:intdot/>=2.3 (CVE-2026-89208)
- TALON TC Compact (BACnet) vers:intdot/<3.5.7 (CVE-2026-102073, CVE-2026-102074, CVE-2026-102075, CVE-2026-102076)
- TALON TC Modular (BACnet) vers:intdot/<3.5.7 (CVE-2026-102073, CVE-2026-102074, CVE-2026-102075, CVE-2026-102076)

Mitigations

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

- CVE-2026-89208 - Apply network segmentation and put the controllers behind properly configured gateways/firewalls.
- Disable the FTP/Web service (Note that the FTP/Web service is disabled by default on APOGEE, Desigo, and TALON products.)

Siemens SIMATIC IPCs

CVE-2026-72895

CVSS 3.1 Score: **7.7**

A BIOS vendor test key is present in the UEFI Secure Boot key database. This could allow a local attacker with physical or administrative access to the device to boot an operating system or UEFI application signed with that test key, bypassing UEFI Secure Boot protections even when Secure Boot is enabled, potentially leading to a full loss of confidentiality, integrity, and availability of the device.

Affected Products

Affected Product and Versions	Remediation
SIMATIC IPC BX-21A < V31.01.13	Update to V31.01.13 or later version
SIMATIC IPC RW-543A < V1.1.4	Update to V1.1.4 or later version
SIMATIC IPC227G / IPC277G / IPC277G PRO / IPC327G / IPC377G < V28.01.15	Update to V28.01.15 or later version

Siemens PSS(R)SINCAL

CVE-2026-84854
CVSS 3.1 Score: **7**

In the WibuKey driver, insufficient validation of user input when calculating the size of a kernel buffer could cause small amounts of data to be written outside the intended kernel buffer. This can lead to a system crash. Under unfavorable circumstances, adjacent kernel memory may be modified.

Affected Products

Affected Product and Versions	Remediation
PSS(R)SINCAL V21.5	Currently no fix is available
PSS(R)SINCAL V22.0	Currently no fix is available
PSS(R)SINCAL V22.5 < V22.5 Update 5	Update to V22.5 Update 5 or later version

Siemens SENTRON 3NA COM Fuse

CVE-2024-7322
CVSS 3.1 Score: **5.8**

A ZigBee coordinator, router, or end device may change their node ID when an unsolicited encrypted rejoin response is received, this change in node ID causes Denial of Service (DoS). To recover from this DoS, the network must be re-established

Affected Products

Affected Product and Versions	Remediation
SENTRON 3NA COM Fuse < V5.2	Update to V5.2 or later version

Siemens Capital Embedded AR Classic

CVE-2026-89208
CVSS 3.1 Score: **5.3**

The affected product does not properly validate input bounds before accessing packet data. This could allow an unauthenticated remote attacker to trigger memory reads outside the intended packet boundaries.

Affected Products

Affected Product and Versions	Remediation
Capital Embedded AR Classic 431-422	Currently no fix is planned
Capital Embedded AR Classic R20-11 < V2303	Update to V2303 or later version

Siemens Software Center

CVE-2026-110936
CVSS 3.1 Score: **6.7**

The affected application loads dynamic-link libraries (DLLs) from an uncontrolled search path. This could allow an authenticated local attacker to place a specially crafted DLL in a directory that the application searches, leading to arbitrary code execution with the privileges of the affected application.

Affected Products

Affected Product and Versions	Remediation
Siemens Software Center < V4.0.9.8	Update to V4.0.9.8 or later version (All existing versions of SSC will be auto updated on next startup. The latest version can also be downloaded in the respective link)

Siemens Industrial Edge App Publisher

CVE-2026-78556
CVSS 3.1 Score: **7.4**

The affected software does not properly validate the server certificate when initiating a TLS connection. This allows an attacker to intercept and relay communication (Man-in-the-Middle attack) and to spoof a trusted entity by interfering in the communication path between the client and the intended server.

CVE-2026-78557
CVSS 3.1 Score: **8.3**

The application fails to properly sanitize or escape data received from the backend before rendering it in the user interface. Because the front end is integrated with Node.js, this vulnerability allows for the execution of arbitrary JavaScript, which can be leveraged to achieve remote code execution (RCE) on the victim's machine.

Affected Products

Affected Product and Versions	Remediation
Industrial Edge App Publisher < V1.27.9	Update to V1.27.9 or later version

Kiloview E3 NDI Encoder

CVE-2026-109122
CVSS 3.1 Score: **9.1**
CVSS 4.0 Score: **9.4**

The network management service on affected Kiloview E3 NDI encoder firmware fails to sanitize one field used when configuring static routes via the web management API. An authenticated web user with permission to configure static routes can exploit this to execute arbitrary operating system commands as root, and the malicious configuration persists across reboots. Successful exploitation could result in full device compromise, including exposure of stored credentials and cryptographic material.

CVE-2026-111100
CVSS 3.1 Score: **5.3**
CVSS 4.0 Score: **6.9**

The ONVIF device service on the E3 responds to certain informational requests without requiring authentication. A remote, unauthenticated party can retrieve detailed device identifiers along with a list of configured user accounts and their privilege levels. This aids attackers in fingerprinting vulnerable devices and preparing targeted credential attacks.

CVE-2026-96616
CVSS 3.1 Score: **6.5**
CVSS 4.0 Score: **8.3**

Authentication tokens issued by the E3's web management interface on login are given an expiration time far beyond any reasonable session lifetime, effectively making them non-expiring. A token obtained through interception or device compromise remains valid for authenticated access for an extended period.

CVE-2026-105265
CVSS 3.1 Score: **5.3**
CVSS 4.0 Score: **6**

A vulnerability exists in the the time zone parameter and does not properly validate user input, which may allow an authenticated user to cause /etc/localtime to point to a file outside

the intended zoneinfo directory

CVE-2026-110491
CVSS 3.1 Score: **7.5**
CVSS 4.0 Score: **6.9**

The ONVIF service on the E3 can be rendered unresponsive by sending malformed or incomplete requests to certain operations. The affected service stops accepting new connections while the rest of the device continues operating normally, and will recover automatically after a period. This can be triggered repeatedly by any unauthenticated party with network access to the device.

CVE-2026-107861
CVSS 3.1 Score: **9.9**
CVSS 4.0 Score: **9.4**

The system control service on affected Kiloview E3 NDI encoder firmware fails to sanitize the hostname parameter accepted by its device naming endpoint, passing it unquoted into a shell command. An authenticated web user with access to this function can embed characters to execute arbitrary operating system commands as root, resulting in full device compromise.

CVE-2026-110243
CVSS 3.1 Score: **9.9**
CVSS 4.0 Score: **9.4**

The network management service on affected Kiloview E3 NDI encoder firmware fails to validate the network interface name accepted by its link maintenance address configuration endpoint before passing it to a shell command, unlike sibling handlers that perform the same validation. An authenticated web user with permission to configure network settings can exploit this to execute arbitrary operating system commands as root.

CVE-2026-92450
CVSS 3.1 Score: **7.5**
CVSS 4.0 Score: **8.7**

The authentication framework used by affected Kiloview E3 NDI encoder firmware signs session JSON Web Tokens using an HMAC-SHA256 secret hardcoded as a static string within the firmware image, identical across all deployed devices. An attacker with access to the publicly distributed firmware can recover this secret and forge arbitrary session tokens, including administrative tokens, without valid credentials, enabling unauthenticated access to privileged device functions.

CVE-2026-110825
CVSS 3.1 Score: **7.5**
CVSS 4.0 Score: **8.7**

The ONVIF device service on affected Kiloview E3 NDI encoder firmware accepts hostname, DNS, and NTP configuration write operations without requiring authentication, regardless of the device's configured authentication setting for this service. A remote, unauthenticated attacker can alter the device hostname, redirect DNS resolution, or modify the configured time source, enabling follow on attacks such as traffic interception or certificate validation bypass.

Affected Products

Affected Product and Versions	Remediation
Kiloview E3 Firmware: <1.30	KiloView recommends users update to V1.30: https://www.kiloview.com/en/download/e3-firmware-downloadlatest-12/

InterSystems Corporation InterSystems IRIS for Health

CVE-2026-111594
CVSS 3.1 Score: **8.1**
CVSS 4.0 Score: **9.2**

InterSystems IRIS for Health has TLS/SSL encryption turned off by default, which may enable an attacker to view transmitted data and use that data to log into the device.

Affected Products

The following versions of InterSystems Corporation InterSystems IRIS for Health are affected:

- InterSystems IRIS for Health 2026.2.0.221, 2026.1.0.235, 2025.3.0.226 (CVE-2026-111594, CVE-2026-111594, CVE-2026-111594)

Mitigations

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

- InterSystems recommends users configure IRIS superserver to require SSL/TLS: https://docs.intersystems.com/irislatest/csp/docbook/DocBook.UI.Page.cls?KEY=ROARS_gsecuring_checklist Note that there are three settings: "Disabled", which means that client communications do not use TLS. "Enabled", which means that client communications may use TLS (but they also may not) and "Required", which forces all client communications to use TLS.
- InterSystems documentation explains how to configure the server to require TLS: https://docs.intersystems.com/irislatest/csp/docbook/DocBook.UI.Page.cls?KEY=GSA_manage_superserver
- For more information about how to configure a system to mitigate this vulnerability, contact InterSystems at their world wide response center: https://wrc.intersystems.com (login required)

References

https://www.cisa.gov/news-events/ics-advisories/icsa-26-295-11
https://www.cisa.gov/news-events/ics-advisories/icsa-26-295-16
https://www.cisa.gov/news-events/ics-advisories/icsa-26-295-18
https://www.cisa.gov/news-events/ics-advisories/icsa-26-295-17
https://www.cisa.gov/news-events/ics-advisories/icsa-26-295-15
https://www.cisa.gov/news-events/ics-advisories/icsa-26-295-14
https://www.cisa.gov/news-events/ics-advisories/icsa-26-295-13
https://www.cisa.gov/news-events/ics-advisories/icsa-26-295-12
https://www.cisa.gov/news-events/ics-advisories/icsa-26-295-10
https://www.cisa.gov/news-events/ics-advisories/icsa-26-295-09
https://www.cisa.gov/news-events/ics-advisories/icsa-26-295-08
https://www.cisa.gov/news-events/ics-advisories/icsa-26-295-07
https://www.cisa.gov/news-events/ics-advisories/icsa-26-295-06
https://www.cisa.gov/news-events/ics-advisories/icsa-26-295-05
https://www.cisa.gov/news-events/ics-advisories/icsa-26-295-04
https://www.cisa.gov/news-events/ics-advisories/icsa-26-295-03
https://www.cisa.gov/news-events/ics-advisories/icsa-26-295-02
https://www.cisa.gov/news-events/ics-advisories/icsa-26-295-01

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com