Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0382

Kwetsbaarheden verholpen in Siemens producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 09-12-2025

TLP:WHITE

Toegestane verspreiding van TLP:WHITE
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Siemens heeft kwetsbaarheden verholpen in diverse producten als Building X, COMOS, Energy Services, Gridscale X, NX, RUGGEDCOM, SICAM, SIMATIC, SINEC, SINEMA, SIPLUS en Solid Edge.

Duiding

De kwetsbaarheden stellen een kwaadwillende mogelijk in staat aanvallen uit te voeren die kunnen leiden tot de volgende categorieën schade:

- Denial-of-Service (DoS)
- Manipulatie van gegevens
- Omzeilen van een beveiligingsmaatregel
- (Remote) code execution (root/admin rechten)
- Toegang tot systeemgegevens
- Toegang tot gevoelige gegevens
- Verhogen van rechten

De kwaadwillende heeft hiervoor toegang nodig tot de productieomgeving. Het is goed gebruik een dergelijke omgeving niet publiek toegankelijk te hebben.

Oplossingen

Siemens heeft beveiligingsupdates uitgebracht om de kwetsbaarheden te verhelpen. Voor de kwetsbaarheden waar nog geen updates voor zijn, heeft Siemens mitigerende maatregelen gepubliceerd om de risico's zoveel als mogelijk te beperken. Zie de bijgevoegde referenties voor meer informatie.

Referenties

- https://cert-portal.siemens.com/productcert/html/ssa-202008.html
- https://cert-portal.siemens.com/productcert/html/ssa-212953.html
- https://cert-portal.siemens.com/productcert/html/ssa-356310.html
- https://cert-portal.siemens.com/productcert/html/ssa-416652.html
- https://cert-portal.siemens.com/productcert/html/ssa-420375.html
- https://cert-portal.siemens.com/productcert/html/ssa-471761.html
- https://cert-portal.siemens.com/productcert/html/ssa-626856.html
- https://cert-portal.siemens.com/productcert/html/ssa-710408.html
- https://cert-portal.siemens.com/productcert/html/ssa-734261.html
- https://cert-portal.siemens.com/productcert/html/ssa-763474.html
- https://cert-portal.siemens.com/productcert/html/ssa-868571.html
- https://cert-portal.siemens.com/productcert/html/ssa-882673.html

- https://cert-portal.siemens.com/productcert/html/ssa-912274.html
- https://cert-portal.siemens.com/productcert/html/ssa-915282.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2018-7169	5.3 MEDIUM
CVE-2018-9234	7.5 HIGH
CVE-2018-12934	7.5 HIGH
CVE-2019-9893	9.8 CRITICAL
CVE-2019-12900	9.8 CRITICAL
CVE-2019-14866	7.3 HIGH
CVE-2020-12762	7.8 HIGH
CVE-2020-21047	5.5 MEDIUM
CVE-2020-22217	5.9 MEDIUM
CVE-2020-35525	7.5 HIGH
CVE-2021-35550	5.9 MEDIUM
CVE-2021-35556	5.3 MEDIUM
CVE-2021-35559	5.3 MEDIUM
CVE-2021-35561	5.3 MEDIUM
CVE-2021-35564	5.3 MEDIUM
CVE-2021-35565	5.3 MEDIUM
CVE-2021-35567	6.8 MEDIUM
CVE-2021-35578	5.3 MEDIUM
CVE-2021-35586	5.3 MEDIUM

CVE-2021-35588	3.1 LOW
CVE-2021-35603	3.7 LOW
CVE-2021-36084	3.3 LOW
CVE-2021-36085	3.3 LOW
CVE-2021-36086	3.3 LOW
CVE-2021-36087	3.3 LOW
CVE-2021-38185	7.8 HIGH
CVE-2021-47358	7.8 HIGH
CVE-2021-47361	7.8 HIGH
CVE-2022-0435	8.8 HIGH
CVE-2022-0492	7.8 HIGH
CVE-2022-0847	7.8 HIGH
CVE-2022-0850	7.1 HIGH
CVE-2022-1353	7.1 HIGH
CVE-2022-1734	7.0 HIGH
CVE-2022-2639	7.8 HIGH
CVE-2022-2964	7.8 HIGH
CVE-2022-3424	7.8 HIGH
CVE-2022-20141	7.0 HIGH
CVE-2022-23039	7.0 HIGH
CVE-2022-23040	7.0 HIGH
CVE-2022-24958	7.8 HIGH
CVE-2022-27223	8.8 HIGH

CVE-2022-28390	7.8 HIGH
CVE-2022-29872	8.7 HIGH
CVE-2022-29873	9.3 CRITICAL
CVE-2022-29874	8.8 HIGH
CVE-2022-29876	7.1 HIGH
CVE-2022-29878	7.5 HIGH
CVE-2022-29879	5.3 MEDIUM
CVE-2022-29880	6.5 MEDIUM
CVE-2022-29881	6.9 MEDIUM
CVE-2022-29882	7.1 HIGH
CVE-2022-29883	6.9 MEDIUM
CVE-2022-30594	7.8 HIGH
CVE-2022-31807	8.2 HIGH
CVE-2022-34903	6.5 MEDIUM
CVE-2022-36123	7.8 HIGH
CVE-2022-37032	9.1 CRITICAL
CVE-2022-37434	9.8 CRITICAL
CVE-2022-40226	7.5 HIGH
CVE-2022-41665	9.8 CRITICAL
CVE-2022-41858	7.1 HIGH
CVE-2022-43439	9.9 CRITICAL
CVE-2022-48624	8.4 HIGH
CVE-2022-48626	7.8 HIGH

CVE-2022-48919	7.5 HIGH
CVE-2022-48926	2.1 LOW
CVE-2022-48948	7.8 HIGH
CVE-2022-48951	7.8 HIGH
CVE-2022-48960	7.8 HIGH
CVE-2022-48962	7.8 HIGH
CVE-2022-48966	7.1 HIGH
CVE-2022-48967	7.1 HIGH
CVE-2022-49058	7.8 HIGH
CVE-2023-4641	5.5 MEDIUM
CVE-2023-27043	5.3 MEDIUM
CVE-2023-28322	9.1 CRITICAL
CVE-2023-29383	3.3 LOW
CVE-2023-29491	7.8 HIGH
CVE-2023-30901	4.3 MEDIUM
CVE-2023-31238	5.5 MEDIUM
CVE-2023-41358	7.5 HIGH
CVE-2023-46218	6.5 MEDIUM
CVE-2023-46753	5.9 MEDIUM
CVE-2023-47234	7.5 HIGH
CVE-2024-0397	7.5 HIGH
CVE-2024-5642	6.5 MEDIUM
CVE-2024-6232	6.9 MEDIUM

CVE-2024-6923	5.1 MEDIUM
CVE-2024-7592	5.1 MEDIUM
CVE-2024-11053	9.1 CRITICAL
CVE-2024-11168	6.3 MEDIUM
CVE-2024-12133	6.9 MEDIUM
CVE-2024-12243	6.9 MEDIUM
CVE-2024-28085	8.8 HIGH
CVE-2024-32487	8.8 HIGH
CVE-2024-47875	7.9 HIGH
CVE-2024-50602	5.1 MEDIUM
CVE-2024-52533	5.1 MEDIUM
CVE-2024-56835	8.7 HIGH
CVE-2024-56836	7.7 HIGH
CVE-2024-56837	8.6 HIGH
CVE-2024-56838	8.6 HIGH
CVE-2024-56839	8.6 HIGH
CVE-2024-56840	7.5 HIGH
CVE-2025-0938	6.3 MEDIUM
CVE-2025-2783	7.6 HIGH
CVE-2025-10148	6.3 MEDIUM
CVE-2025-40800	9.1 CRITICAL
CVE-2025-40801	9.2 CRITICAL
CVE-2025-40806	6.9 MEDIUM

CVE-2025-40807	5.3 MEDIUM
CVE-2025-40818	4.8 MEDIUM
CVE-2025-40819	5.3 MEDIUM
CVE-2025-40820	8.7 HIGH
CVE-2025-40830	8.4 HIGH
CVE-2025-40831	7.1 HIGH
CVE-2025-40935	5.3 MEDIUM
CVE-2025-40938	9.2 CRITICAL
CVE-2025-40939	5.1 MEDIUM
CVE-2025-40940	6.9 MEDIUM
CVE-2025-40941	5.3 MEDIUM
CVE-2025-59392	6.8 MEDIUM
CVE-2018-1000876	7.8 HIGH

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
CWE-74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-94	Improper Control of Generation of Code ('Code Injection')

CWE-96	Improper Neutralization of Directives in Statically Saved Code ('Static Code Injection')
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-121	Stack-based Buffer Overflow
CWE-125	Out-of-bounds Read
CWE-126	Buffer Over-read
CWE-129	Improper Validation of Array Index
CWE-141	Improper Neutralization of Parameter/Argument Delimiters
CWE-150	Improper Neutralization of Escape, Meta, or Control Sequences
CWE-178	Improper Handling of Case Sensitivity
CWE-190	Integer Overflow or Wraparound
CWE-191	Integer Underflow (Wrap or Wraparound)
CWE-192	Integer Coercion Error
CWE-193	Off-by-one Error
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-201	Insertion of Sensitive Information Into Sent Data
CWE-203	Observable Discrepancy
CWE-204	Observable Response Discrepancy
CWE-212	Improper Removal of Sensitive Information Before Storage or Transfer
CWE-264	CWE-264
CWE-268	Privilege Chaining
CWE-271	Privilege Dropping / Lowering Errors
CWE-276	Incorrect Default Permissions
CWE-281	Improper Preservation of Permissions
CWE-284	Improper Access Control

CWE-285	Improper Authorization
CWE-287	Improper Authentication
CWE-288	Authentication Bypass Using an Alternate Path or Channel
CWE-294	Authentication Bypass by Capture-replay
CWE-295	Improper Certificate Validation
CWE-303	Incorrect Implementation of Authentication Algorithm
CWE-306	Missing Authentication for Critical Function
CWE-310	CWE-310
CWE-311	Missing Encryption of Sensitive Data
CWE-319	Cleartext Transmission of Sensitive Information
CWE-327	Use of a Broken or Risky Cryptographic Algorithm
CWE-328	Use of Weak Hash
CWE-340	Generation of Predictable Numbers or Identifiers
CWE-347	Improper Verification of Cryptographic Signature
CWE-352	Cross-Site Request Forgery (CSRF)
CWE-354	Improper Validation of Integrity Check Value
CWE-358	Improperly Implemented Security Check for Standard
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-384	Session Fixation
CWE-385	Covert Timing Channel
CWE-399	CWE-399
CWE-400	Uncontrolled Resource Consumption
CWE-404	Improper Resource Shutdown or Release
CWE-407	Inefficient Algorithmic Complexity
CWE-414	Missing Lock Check

CWE-415	Double Free
CWE-416	Use After Free
CWE-440	Expected Behavior Violation
CWE-476	NULL Pointer Dereference
CWE-502	Deserialization of Untrusted Data
CWE-665	Improper Initialization
CWE-667	Improper Locking
CWE-668	Exposure of Resource to Wrong Sphere
CWE-681	Incorrect Conversion between Numeric Types
CWE-732	Incorrect Permission Assignment for Critical Resource
CWE-754	Improper Check for Unusual or Exceptional Conditions
CWE-763	Release of Invalid Pointer or Reference
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-787	Out-of-bounds Write
CWE-798	Use of Hard-coded Credentials
CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')
CWE-862	Missing Authorization
CWE-863	Incorrect Authorization
CWE-909	Missing Initialization of Resource
CWE-918	Server-Side Request Forgery (SSRF)
CWE-940	Improper Verification of Source of a Communication Channel
CWE-1214	CWE-1214
CWE-1287	Improper Validation of Specified Type of Input
CWE-1333	Inefficient Regular Expression Complexity

Getroffen producten

Siemens
Building X - Security Manager Edge Controller (ACC-AP)
COMOS V10.4
COMOS V10.4.5
COMOS V10.5
COMOS V10.5.2
COMOS V10.6
Energy Services
Gridscale X Prepay
NX V2412
NX V2506
SICAM
SIMATIC CFU DIQ
SIMATIC CFU PA
SIMATIC CN 4100
SIMATIC ET 200AL IM 157-1 PN

SIMATIC MV540 H Firmware
SIMATIC PN/PN Coupler
SIMATIC S7
SINEC INS
SINEC NMS
SINEC PNI
SINEMA Remote Connect Server
SIPLUS ET 200MP IM 155-5 PN HF
SIPLUS HCS4200 CIM4210
SIPLUS NET PN/PN Coupler
SIPLUS S7-1200 CPU 1212 AC/DC/RLY
SIPLUS S7-1200 CPU 1214 AC/DC/RLY
SIPLUS S7-1200 CPU 1215 AC/DC/RLY
SIPLUS S7-1500 CPU 1511-1 PN
SIPLUS S7-300 CPU 314C-2 PN/DP
Solid Edge SE2025

Solid Edge
SE2026

Disclaimer