Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0061

Kwetsbaarheden verholpen in Siemens producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 14-02-2025

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 APOGEE, Opcenter, RUGGEDCOM, SCALANCE, SIMATIC, SIPROTEC en Teamcenter.

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)
- Cross-Site-Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Manipulatie van gegevens
- Omzeilen van een beveiligingsmaatregel
- Omzeilen van authenticatie
- (Remote) code execution (root/admin rechten)
- (Remote) code execution (Gebruikersrechten)
- Toegang tot systeemgegevens
- Toegang tot gevoelige gegevens

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/pdf/ssa-111547.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-195895.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-224824.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-246355.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-342348.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-369369.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-615116.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-637914.pdf

- https://cert-portal.siemens.com/productcert/pdf/ssa-647005.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-656895.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-687955.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-767615.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-769027.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-770770.pdf

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-46665	3.7 LOW
CVE-2024-46666	5.3 MEDIUM
CVE-2024-46668	7.5 HIGH
CVE-2024-46669	
CVE-2024-46670	7.5 HIGH
CVE-2024-48884	
CVE-2024-48885	2.3 LOW
CVE-2024-50560	2.3 LOW
CVE-2024-50561	5.1 MEDIUM
CVE-2024-50572	8.6 HIGH
CVE-2024-52963	
CVE-2024-53648	7.0 HIGH
CVE-2024-53651	5.1 MEDIUM
CVE-2024-53977	7.3 HIGH
CVE-2024-54015	8.7 HIGH
CVE-2024-54021	
CVE-2024-54089	8.7 HIGH

CVE-2024-54090	6.3 MEDIUM
CVE-2025-23363	6.3 MEDIUM
CVE-2025-23403	7.3 HIGH
CVE-2025-24499	7.5 HIGH
CVE-2025-24532	5.3 MEDIUM
CVE-2025-24811	8.7 HIGH
CVE-2025-24812	7.1 HIGH
CVE-2025-24956	6.9 MEDIUM
CVE-2022-2588	7.8 HIGH
CVE-2022-2663	
CVE-2022-3524	
CVE-2022-4304	7.5 HIGH
CVE-2022-4450	7.5 HIGH
CVE-2022-22127	7.7 HIGH
CVE-2022-22128	9.0 CRITICAL
CVE-2022-39188	
CVE-2022-39842	6.1 MEDIUM
CVE-2022-40303	7.8 HIGH
CVE-2022-40304	7.8 HIGH
CVE-2022-43750	
CVE-2022-47069	7.8 HIGH
CVE-2022-47929	5.5 MEDIUM
CVE-2023-0045	

CVE-2023-0215	7.5 HIGH
CVE-2023-0286	7.5 HIGH
CVE-2023-0464	7.8 HIGH
CVE-2023-0465	7.8 HIGH
CVE-2023-0466	7.8 HIGH
CVE-2023-0590	7.0 HIGH
CVE-2023-1073	6.6 MEDIUM
CVE-2023-1074	5.5 MEDIUM
CVE-2023-1118	7.8 HIGH
CVE-2023-1206	5.7 MEDIUM
CVE-2023-1380	7.1 HIGH
CVE-2023-1670	7.8 HIGH
CVE-2023-2194	6.7 MEDIUM
CVE-2023-3446	7.8 HIGH
CVE-2023-3611	7.8 HIGH
CVE-2023-4623	7.8 HIGH
CVE-2023-4921	7.8 HIGH
CVE-2023-5363	7.5 HIGH
CVE-2023-5678	
CVE-2023-5717	7.8 HIGH
CVE-2023-6129	6.5 MEDIUM
CVE-2023-6237	5.9 MEDIUM
CVE-2023-7250	5.3 MEDIUM

CVE-2023-23454	5.5 MEDIUM
CVE-2023-23455	
CVE-2023-23559	7.8 HIGH
CVE-2023-26545	
CVE-2023-28484	6.5 MEDIUM
CVE-2023-28578	9.3 CRITICAL
CVE-2023-29469	6.5 MEDIUM
CVE-2023-31085	5.5 MEDIUM
CVE-2023-31315	7.1 HIGH
CVE-2023-35001	
CVE-2023-37482	6.9 MEDIUM
CVE-2023-39192	6.7 MEDIUM
CVE-2023-39193	6.1 MEDIUM
CVE-2023-42754	5.5 MEDIUM
CVE-2023-43522	7.5 HIGH
CVE-2023-44320	4.3 MEDIUM
CVE-2023-44322	3.7 LOW
CVE-2023-45853	9.8 CRITICAL
CVE-2023-45863	6.4 MEDIUM
CVE-2023-46604	10.0 CRITICAL
CVE-2023-48795	7.5 HIGH
CVE-2023-51384	5.9 MEDIUM
CVE-2023-51385	6.5 MEDIUM

CVE-2024-0727	7.5 HIGH
CVE-2024-2511	9.1 CRITICAL
CVE-2024-4603	9.1 CRITICAL
CVE-2024-4741	
CVE-2024-5535	9.1 CRITICAL
CVE-2024-6119	9.1 CRITICAL
CVE-2024-9143	6.9 MEDIUM
CVE-2024-23814	6.9 MEDIUM
CVE-2024-26306	5.9 MEDIUM
CVE-2024-33016	7.0 HIGH
CVE-2024-36504	6.5 MEDIUM
CVE-2024-45386	8.7 HIGH

CWE's

CWE	Beschrijving
CWE-1240	Use of a Cryptographic Primitive with a Risky Implementation
CWE-1325	Improperly Controlled Sequential Memory Allocation
CWE-468	Incorrect Pointer Scaling
CWE-606	Unchecked Input for Loop Condition
CWE-183	Permissive List of Allowed Inputs
CWE-385	Covert Timing Channel
CWE-1395	Dependency on Vulnerable Third-Party Component
CWE-170	Improper Null Termination
CWE-489	Active Debug Code

CWE-1392	Use of Default Credentials
CWE-222	Truncation of Security-relevant Information
CWE-310	CWE-310
CWE-328	Use of Weak Hash
CWE-304	Missing Critical Step in Authentication
CWE-684	Incorrect Provision of Specified Functionality
CWE-208	Observable Timing Discrepancy
CWE-326	Inadequate Encryption Strength
CWE-923	Improper Restriction of Communication Channel to Intended Endpoints
CWE-201	Insertion of Sensitive Information Into Sent Data
CWE-347	Improper Verification of Cryptographic Signature
CWE-834	Excessive Iteration
CWE-732	Incorrect Permission Assignment for Critical Resource
CWE-425	Direct Request ('Forced Browsing')
CWE-440	Expected Behavior Violation
CWE-704	Incorrect Type Conversion or Cast
CWE-415	Double Free
CWE-1286	Improper Validation of Syntactic Correctness of Input
CWE-754	Improper Check for Unusual or Exceptional Conditions
CWE-427	Uncontrolled Search Path Element
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')
CWE-610	Externally Controlled Reference to a Resource in Another Sphere
CWE-613	Insufficient Session Expiration
CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')
CWE-312	Cleartext Storage of Sensitive Information
CWE-369	Divide By Zero

CWE-252	Unchecked Return Value
CWE-203	Observable Discrepancy
CWE-354	Improper Validation of Integrity Check Value
CWE-325	Missing Cryptographic Step
CWE-190	Integer Overflow or Wraparound
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-125	Out-of-bounds Read
CWE-404	Improper Resource Shutdown or Release
CWE-284	Improper Access Control
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
CWE-1333	Inefficient Regular Expression Complexity
CWE-416	Use After Free
CWE-113	Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting')
CWE-401	Missing Release of Memory after Effective Lifetime
CWE-476	NULL Pointer Dereference
CWE-295	Improper Certificate Validation
CWE-757	Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade')
CWE-327	Use of a Broken or Risky Cryptographic Algorithm
CWE-436	Interpretation Conflict
CWE-400	Uncontrolled Resource Consumption

Getroffen producten

siemens
apogee_pxc_series__bacnet_
apogee_pxc_series__p2_ethernet_
opcenter_intelligence
ruggedcom
scalance
_simatic_s7
_simatic
simatic_s7
simatic
siprotec
teamcenter

Disclaimer