Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0147

Kwetsbaarheden verholpen in Siemens-producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 13-05-2026

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 verschillende (OT-)producten. Het gaat onder andere om producten in de Siemens RUGGEDCOM-, SCALANCE-, SIMATIC-, SIMIT-, SINAMICS-, SIPROTEC-, SENTRON- en Solid Edge-productreeksen.

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
- (Remote) code execution
- Toegang tot gevoelige gegevens
- Verhogen van rechten

Voor succesvol misbruik van de genoemde kwetsbaarheden moet de kwaadwillende (netwerk)toegang hebben tot het kwetsbare product. Het is goed gebruik een dergelijke producten 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-032379.html
- https://cert-portal.siemens.com/productcert/html/ssa-078743.html
- https://cert-portal.siemens.com/productcert/html/ssa-081142.html
- https://cert-portal.siemens.com/productcert/html/ssa-085541.html
- https://cert-portal.siemens.com/productcert/html/ssa-357982.html
- https://cert-portal.siemens.com/productcert/html/ssa-387223.html
- https://cert-portal.siemens.com/productcert/html/ssa-392349.html
- https://cert-portal.siemens.com/productcert/html/ssa-545643.html
- https://cert-portal.siemens.com/productcert/html/ssa-577017.html
- https://cert-portal.siemens.com/productcert/html/ssa-688146.html
- https://cert-portal.siemens.com/productcert/html/ssa-783943.html
- https://cert-portal.siemens.com/productcert/html/ssa-786884.html
- https://cert-portal.siemens.com/productcert/html/ssa-827383.html

- https://cert-portal.siemens.com/productcert/html/ssa-870926.html
- https://cert-portal.siemens.com/productcert/html/ssa-876049.html
- https://cert-portal.siemens.com/productcert/html/ssa-921111.html
- https://cert-portal.siemens.com/productcert/html/ssa-973901.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2019-13103	7.1 HIGH
CVE-2019-13104	7.8 HIGH
CVE-2019-13106	7.8 HIGH
CVE-2019-14192	9.8 CRITICAL
CVE-2019-14193	9.8 CRITICAL
CVE-2019-14194	9.8 CRITICAL
CVE-2019-14195	9.8 CRITICAL
CVE-2019-14196	9.8 CRITICAL
CVE-2019-14197	9.1 CRITICAL
CVE-2019-14198	9.8 CRITICAL
CVE-2019-14199	9.8 CRITICAL
CVE-2019-14200	9.8 CRITICAL
CVE-2019-14201	9.8 CRITICAL
CVE-2019-14202	9.8 CRITICAL
CVE-2019-14203	9.8 CRITICAL
CVE-2019-14204	9.8 CRITICAL
CVE-2020-10648	7.8 HIGH
CVE-2022-2347	7.7 HIGH

CVE-2022-30552	6.2 MEDIUM
CVE-2022-30790	7.8 HIGH
CVE-2022-34835	9.8 CRITICAL
CVE-2023-3019	6.5 MEDIUM
CVE-2023-27043	5.3 MEDIUM
CVE-2024-3447	6.0 MEDIUM
CVE-2024-4367	8.8 HIGH
CVE-2024-22365	5.5 MEDIUM
CVE-2024-47704	5.5 MEDIUM
CVE-2024-54017	6.9 MEDIUM
CVE-2024-57256	8.5 HIGH
CVE-2024-57258	8.5 HIGH
CVE-2024-57924	5.5 MEDIUM
CVE-2024-58240	5.9 MEDIUM
CVE-2025-0395	7.5 HIGH
CVE-2025-3576	5.9 MEDIUM
CVE-2025-6020	8.5 HIGH
CVE-2025-6021	5.3 MEDIUM
CVE-2025-6052	5.1 MEDIUM
CVE-2025-7425	2.0 LOW
CVE-2025-8916	6.3 MEDIUM
CVE-2025-9230	6.9 MEDIUM
CVE-2025-9231	6.3 MEDIUM

CVE-2025-9232	6.3 MEDIUM
CVE-2025-9714	6.2 MEDIUM
CVE-2025-9820	5.3 MEDIUM
CVE-2025-12659	7.3 HIGH
CVE-2025-14831	5.3 MEDIUM
CVE-2025-22871	6.9 MEDIUM
CVE-2025-23143	5.5 MEDIUM
CVE-2025-23160	5.5 MEDIUM
CVE-2025-31257	2.3 LOW
CVE-2025-37931	5.5 MEDIUM
CVE-2025-37968	7.0 HIGH
CVE-2025-38322	5.9 MEDIUM
CVE-2025-38347	5.9 MEDIUM
CVE-2025-38491	5.9 MEDIUM
CVE-2025-38502	5.1 MEDIUM
CVE-2025-38552	2.1 LOW
CVE-2025-38614	6.2 MEDIUM
CVE-2025-38670	7.1 HIGH
CVE-2025-38676	7.8 HIGH
CVE-2025-38677	5.1 MEDIUM
CVE-2025-38679	7.1 HIGH
CVE-2025-38680	7.1 HIGH
CVE-2025-38681	6.5 MEDIUM

CVE-2025-38683	7.0 HIGH
CVE-2025-38684	7.0 HIGH
CVE-2025-38685	7.8 HIGH
CVE-2025-38687	5.5 MEDIUM
CVE-2025-38691	5.5 MEDIUM
CVE-2025-38693	7.0 HIGH
CVE-2025-38694	7.0 HIGH
CVE-2025-38695	7.0 HIGH
CVE-2025-38696	5.5 MEDIUM
CVE-2025-38697	7.8 HIGH
CVE-2025-38698	7.1 HIGH
CVE-2025-38699	7.8 HIGH
CVE-2025-38700	7.0 HIGH
CVE-2025-38701	7.0 HIGH
CVE-2025-38702	7.8 HIGH
CVE-2025-38706	7.0 HIGH
CVE-2025-38707	7.8 HIGH
CVE-2025-38708	7.8 HIGH
CVE-2025-38711	5.5 MEDIUM
CVE-2025-38712	5.5 MEDIUM
CVE-2025-38713	7.1 HIGH
CVE-2025-38714	9.0 CRITICAL
CVE-2025-38715	7.1 HIGH

CVE-2025-38721	5.5 MEDIUM
CVE-2025-38723	5.5 MEDIUM
CVE-2025-38724	7.8 HIGH
CVE-2025-38725	7.0 HIGH
CVE-2025-38727	5.5 MEDIUM
CVE-2025-38728	7.1 HIGH
CVE-2025-38729	7.8 HIGH
CVE-2025-38732	7.5 HIGH
CVE-2025-38735	7.0 HIGH
CVE-2025-38736	7.1 HIGH
CVE-2025-39673	7.0 HIGH
CVE-2025-39675	5.5 MEDIUM
CVE-2025-39676	5.5 MEDIUM
CVE-2025-39681	5.5 MEDIUM
CVE-2025-39682	7.1 HIGH
CVE-2025-39683	7.1 HIGH
CVE-2025-39684	5.5 MEDIUM
CVE-2025-39685	7.1 HIGH
CVE-2025-39686	7.8 HIGH
CVE-2025-39687	7.1 HIGH
CVE-2025-39689	7.8 HIGH
CVE-2025-39691	7.8 HIGH
CVE-2025-39692	5.5 MEDIUM

CVE-2025-39693	5.5 MEDIUM
CVE-2025-39694	7.0 HIGH
CVE-2025-39697	7.5 HIGH
CVE-2025-39701	7.8 HIGH
CVE-2025-39702	7.1 HIGH
CVE-2025-39703	7.0 HIGH
CVE-2025-39706	5.5 MEDIUM
CVE-2025-39709	5.5 MEDIUM
CVE-2025-39710	7.1 HIGH
CVE-2025-39713	7.0 HIGH
CVE-2025-39714	5.5 MEDIUM
CVE-2025-39715	5.5 MEDIUM
CVE-2025-39716	5.5 MEDIUM
CVE-2025-39718	7.6 HIGH
CVE-2025-39719	5.1 MEDIUM
CVE-2025-39724	8.6 HIGH
CVE-2025-39736	5.5 MEDIUM
CVE-2025-39737	5.5 MEDIUM
CVE-2025-39738	7.8 HIGH
CVE-2025-39742	7.0 HIGH
CVE-2025-39743	9.8 CRITICAL
CVE-2025-39749	7.0 HIGH
CVE-2025-39752	5.5 MEDIUM

CVE-2025-39756	5.5 MEDIUM
CVE-2025-39757	7.8 HIGH
CVE-2025-39759	7.0 HIGH
CVE-2025-39760	8.6 HIGH
CVE-2025-39766	7.8 HIGH
CVE-2025-39770	7.0 HIGH
CVE-2025-39772	5.5 MEDIUM
CVE-2025-39773	5.9 MEDIUM
CVE-2025-39776	7.8 HIGH
CVE-2025-39782	8.6 HIGH
CVE-2025-39783	8.6 HIGH
CVE-2025-39787	5.5 MEDIUM
CVE-2025-39788	7.8 HIGH
CVE-2025-39790	7.5 HIGH
CVE-2025-39794	6.9 MEDIUM
CVE-2025-39795	8.6 HIGH
CVE-2025-39798	5.1 MEDIUM
CVE-2025-39800	5.5 MEDIUM
CVE-2025-39801	6.2 MEDIUM
CVE-2025-39806	7.1 HIGH
CVE-2025-39808	5.5 MEDIUM
CVE-2025-39812	5.1 MEDIUM
CVE-2025-39813	5.5 MEDIUM

CVE-2025-39817	2.1 LOW
CVE-2025-39819	5.5 MEDIUM
CVE-2025-39823	8.6 HIGH
CVE-2025-39824	7.8 HIGH
CVE-2025-39825	2.1 LOW
CVE-2025-39826	5.9 MEDIUM
CVE-2025-39827	5.1 MEDIUM
CVE-2025-39828	2.1 LOW
CVE-2025-39835	7.8 HIGH
CVE-2025-39838	7.0 HIGH
CVE-2025-39839	7.1 HIGH
CVE-2025-39841	7.8 HIGH
CVE-2025-39842	5.5 MEDIUM
CVE-2025-39843	7.0 HIGH
CVE-2025-39844	5.5 MEDIUM
CVE-2025-39845	5.5 MEDIUM
CVE-2025-39846	5.5 MEDIUM
CVE-2025-39847	5.5 MEDIUM
CVE-2025-39848	5.5 MEDIUM
CVE-2025-39849	7.8 HIGH
CVE-2025-39853	7.1 HIGH
CVE-2025-39857	7.0 HIGH
CVE-2025-39860	7.8 HIGH

CVE-2025-39864	7.8 HIGH
CVE-2025-39865	7.0 HIGH
CVE-2025-39866	7.8 HIGH
CVE-2025-40300	6.5 MEDIUM
CVE-2025-40833	8.7 HIGH
CVE-2025-40946	7.2 HIGH
CVE-2025-40947	7.7 HIGH
CVE-2025-40948	6.1 MEDIUM
CVE-2025-40949	8.9 HIGH
CVE-2025-43368	5.3 MEDIUM
CVE-2025-46836	6.6 MEDIUM
CVE-2025-47219	5.3 MEDIUM
CVE-2025-48989	6.9 MEDIUM
CVE-2025-49794	5.3 MEDIUM
CVE-2025-49796	5.3 MEDIUM
CVE-2025-53057	5.9 MEDIUM
CVE-2025-53066	7.5 HIGH
CVE-2025-55752	7.7 HIGH
CVE-2025-55754	2.1 LOW
CVE-2025-61748	3.7 LOW
CVE-2025-61795	2.3 LOW
CVE-2026-2673	6.3 MEDIUM
CVE-2026-21925	4.8 MEDIUM

CVE-2026-21932	7.4 HIGH
CVE-2026-21933	6.1 MEDIUM
CVE-2026-21945	7.5 HIGH
CVE-2026-21947	3.1 LOW
CVE-2026-22924	8.8 HIGH
CVE-2026-22925	8.7 HIGH
CVE-2026-25786	9.3 CRITICAL
CVE-2026-25787	9.3 CRITICAL
CVE-2026-25789	7.2 HIGH
CVE-2026-27446	9.3 CRITICAL
CVE-2026-27662	7.0 HIGH
CVE-2026-28387	8.1 HIGH
CVE-2026-28388	7.5 HIGH
CVE-2026-28389	7.5 HIGH
CVE-2026-28390	7.5 HIGH
CVE-2026-31789	9.8 CRITICAL
CVE-2026-31790	7.5 HIGH
CVE-2026-33862	8.5 HIGH
CVE-2026-33893	8.7 HIGH
CVE-2026-40175	6.9 MEDIUM
CVE-2026-41125	5.9 MEDIUM
CVE-2026-41551	9.3 CRITICAL
CVE-2026-44411	8.7 HIGH

CVE-2026-44412	8.7 HIGH

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-23	Relative Path Traversal
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-88	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-93	Improper Neutralization of CRLF Sequences ('CRLF Injection')
CWE-113	Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting')
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-122	Heap-based Buffer Overflow
CWE-125	Out-of-bounds Read
CWE-129	Improper Validation of Array Index
CWE-131	Incorrect Calculation of Buffer Size
CWE-150	Improper Neutralization of Escape, Meta, or Control Sequences
CWE-190	Integer Overflow or Wraparound

CWE-191	Integer Underflow (Wrap or Wraparound)
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-203	Observable Discrepancy
CWE-208	Observable Timing Discrepancy
CWE-273	Improper Check for Dropped Privileges
CWE-277	Insecure Inherited Permissions
CWE-284	Improper Access Control

Getroffen producten

Siemens
IE/PB-Link Firmware (OS)
IE/PB-link Firmware
Opcenter RDnL
RUGGEDCOM ROX II
RUGGEDCOM ROX II Family
RUGGEDCOM ROX II family
SCALANCE M-800
SCALANCE M-800 family
SCALANCE SC-600

SCALANCE SC-600 Family
SCALANCE SC-600 family
SCALANCE W-700 IEEE 802.11n family
SCALANCE X-200 series firmware
SCALANCE X-300 Series Firmware
SCALANCE XM-400
SCALANCE XM-400 Family
SCALANCE XM-400 family
SCALANCE XR-500 Family
SCALANCE XR-500 family
SIMATIC CFU DIQ
SIMATIC CFU PA
SIMATIC ET 200 SP Firmware
SIMATIC HMI Unified Comfort Panels
SIMATIC HMI Unified Comfort Panels Firmware
SIMATIC HMI Unified Comfort Panels family

SIMATIC S7
SIMATIC S7-1500
SIMATIC S7-300
SIMATIC S7-410
SIMIT
SINAMICS G115D
SINAMICS G130
SINAMICS S110
SINAMICS S150
SIPROTEC 5
Scalance W-700 Ieee 80211N Family
Scalance X-200 Firmware
Scalance X-300
Sentron PAC
Simatic S7-400 Firmware
Simcenter Femap

Sinamics G120
Sinamics S120
Solid Edge SE2026
Teamcenter

Siemens AG

SINUMERIK 808D V4.7, SINUMERIK 808D V4.8, SINUMERIK 828D V4.7, SINUMERIK 840D sl V4.7, SINUMERIK 840D sl V4.8

Disclaimer