



NCSC-2026-0187

Kwetsbaarheden verholpen in Siemens producten

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 09-06-2026

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 diverse producten als SCALANCE, SIMATIC, SINAMICS, SIPROTEC en TIA Portal.

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

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-063511.html>
- <https://cert-portal.siemens.com/productcert/html/ssa-139483.html>
- <https://cert-portal.siemens.com/productcert/html/ssa-434797.html>
- <https://cert-portal.siemens.com/productcert/html/ssa-693808.html>
- <https://cert-portal.siemens.com/productcert/html/ssa-860189.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2024-54678	9.3 CRITICAL
➤ CVE-2025-15467	9.8 CRITICAL

> CVE-2025-40808	6.9 MEDIUM
> CVE-2026-24349	8.2 HIGH
> CVE-2026-46746	8.7 HIGH
> CVE-2026-46747	5.3 MEDIUM
> CVE-2026-46748	8.7 HIGH
> CVE-2026-46749	5.0 MEDIUM

CWE's

CWE	Beschrijving
> CWE-26	Path Traversal: '/dir/../../filename'
> CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
> CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
> CWE-250	Execution with Unnecessary Privileges
> CWE-313	Cleartext Storage in a File or on Disk
> CWE-434	Unrestricted Upload of File with Dangerous Type
> CWE-502	Deserialization of Untrusted Data
> CWE-760	Use of a One-Way Hash with a Predictable Salt
> CWE-787	Out-of-bounds Write

Getroffen producten

Siemens
AI Lightweight Inference Server
Connector for Azure

Databus
HiMed Cockpit
RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2)
RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2)
SCALANCE LPE9403 (6GK5998-3GS00-2AC2)
SCALANCE LPE9413 (6GK5998-3GS01-2AC2)
SCALANCE LPE9433 (6GK5998-3GS11-2AC2)
SCALANCE M804PB (6GK5804-0AP00-2AA2)
SCALANCE M812-1 ADSL- Router family
SCALANCE M816-1 ADSL- Router family
SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2)
SCALANCE M874-2 (6GK5874-2AA00-2AA2)
SCALANCE M874-3 (6GK5874-3AA00-2AA2)
SCALANCE M874-3 3G-Router (CN) (6GK5874-3AA00-2FA2)
SCALANCE M876-3 (6GK5876-3AA02-2BA2)
SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2)

SCALANCE M876-4 (6GK5876-4AA10-2BA2)
SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2)
SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2)
SCALANCE MUB852-1 (A1) (6GK5852-1EA10-1AA1)
SCALANCE MUB852-1 (B1) (6GK5852-1EA10-1BA1)
SCALANCE MUM853-1 (A1) (6GK5853-2EA10-2AA1)
SCALANCE MUM853-1 (B1) (6GK5853-2EA10-2BA1)
SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1)
SCALANCE MUM856-1 (A1) (6GK5856-2EA10-3AA1)
SCALANCE MUM856-1 (B1) (6GK5856-2EA10-3BA1)
SCALANCE MUM856-1 (CN) (6GK5856-2EA00-3FA1)
SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1)
SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1)
SCALANCE S615 EEC LAN-Router (6GK5615-0AA01-2AA2)
SCALANCE S615 LAN-Router (6GK5615-0AA00-2AA2)
SCALANCE SC622-2C (6GK5622-2GS00-2AC2)

SCALANCE SC626-2C (6GK5626-2GS00-2AC2)
SCALANCE SC632-2C (6GK5632-2GS00-2AC2)
SCALANCE SC636-2C (6GK5636-2GS00-2AC2)
SCALANCE SC642-2C (6GK5642-2GS00-2AC2)
SCALANCE SC646-2C (6GK5646-2GS00-2AC2)
SCALANCE WAB762-1 (6GK5762-1AJ00-6AA0)
SCALANCE WAM763-1 (6GK5763-1AL00-7DA0)
SCALANCE WAM763-1 (ME) (6GK5763-1AL00-7DC0)
SCALANCE WAM763-1 (US) (6GK5763-1AL00-7DB0)
SCALANCE WAM766-1 (6GK5766-1GE00-7DA0)
SCALANCE WAM766-1 (ME) (6GK5766-1GE00-7DC0)
SCALANCE WAM766-1 (US) (6GK5766-1GE00-7DB0)
SCALANCE WAM766-1 EEC (6GK5766-1GE00-7TA0)
SCALANCE WAM766-1 EEC (ME) (6GK5766-1GE00-7TC0)
SCALANCE WAM766-1 EEC (US) (6GK5766-1GE00-7TB0)
SCALANCE WUB762-1 (6GK5762-1AJ00-1AA0)

SCALANCE WUB762-1 iFeatures
(6GK5762-1AJ00-2AA0)

SCALANCE WUM763-1
(6GK5763-1AL00-3AA0)

SCALANCE WUM763-1
(6GK5763-1AL00-3DA0)

SCALANCE WUM763-1 (US)
(6GK5763-1AL00-3AB0)

SCALANCE WUM763-1 (US)
(6GK5763-1AL00-3DB0)

SCALANCE WUM766-1
(6GK5766-1GE00-3DA0)

SCALANCE WUM766-1 (ME)
(6GK5766-1GE00-3DC0)

SCALANCE WUM766-1 (USA)
(6GK5766-1GE00-3DB0)

SCALANCE XC316-8
(6GK5324-8TS00-2AC2)

SCALANCE XC324-4
(6GK5328-4TS00-2AC2)

SCALANCE XC324-4 EEC
(6GK5328-4TS00-2EC2)

SCALANCE XC332
(6GK5332-0GA00-2AC2)

SCALANCE XC416-8
(6GK5424-8TR00-2AC2)

SCALANCE XC424-4
(6GK5428-4TR00-2AC2)

SCALANCE XC432
(6GK5432-0GR00-2AC2)

SCALANCE XR302-32
(6GK5334-5TS00-2AR3)

SCALANCE XR302-32 (6GK5334-5TS00-3AR3)
SCALANCE XR302-32 (6GK5334-5TS00-4AR3)
SCALANCE XR322-12 (6GK5334-3TS00-2AR3)
SCALANCE XR322-12 (6GK5334-3TS00-3AR3)
SCALANCE XR322-12 (6GK5334-3TS00-4AR3)
SCALANCE XR326-8 (6GK5334-2TS00-2AR3)
SCALANCE XR326-8 (6GK5334-2TS00-3AR3)
SCALANCE XR326-8 (6GK5334-2TS00-4AR3)
SCALANCE XR326-8 EEC (6GK5334-2TS00-2ER3)
SCALANCE XR502-32 (6GK5534-5TR00-2AR3)
SCALANCE XR502-32 (6GK5534-5TR00-3AR3)
SCALANCE XR502-32 (6GK5534-5TR00-4AR3)
SCALANCE XR522-12 (6GK5534-3TR00-2AR3)
SCALANCE XR522-12 (6GK5534-3TR00-3AR3)
SCALANCE XR522-12 (6GK5534-3TR00-4AR3)
SCALANCE XR524-8WG (6GK5532-2SR00-2AR3)

SCALANCE XR524-8WG (6GK5532-2SR00-2RR3)
SCALANCE XR524-8WG (6GK5532-2SR00-3AR3)
SCALANCE XR524-8WG (6GK5532-2SR00-3RR3)
SCALANCE XR526-8 (6GK5534-2TR00-2AR3)
SCALANCE XR526-8 (6GK5534-2TR00-3AR3)
SCALANCE XR526-8 (6GK5534-2TR00-4AR3)
SIDIS Prime
SIMATIC Comfort/ Mobile RT
SIMATIC HMI Basic Panels
SIMATIC HMI Comfort Panels
SIMATIC HMI Mobile Panels
SIMATIC IOT2050 (6ES7647-0BA00-1YA2)
SIMATIC IPC BX-21A
SIMATIC IPC MD-57A
SIMATIC IPC ORCLA
SIMATIC PCS neo

SIMATIC PCS neo V4.1
SIMATIC PCS neo V5.0
SIMATIC PCS neo V6.0
SIMATIC PDM V9.3
SIMATIC RTLS Locating Manager (6GT2780-0DA00)
SIMATIC RTLS Locating Manager (6GT2780-0DA10)
SIMATIC RTLS Locating Manager (6GT2780-0DA20)
SIMATIC RTLS Locating Manager (6GT2780-0DA30)
SIMATIC RTLS Locating Manager (6GT2780-1EA10)
SIMATIC RTLS Locating Manager (6GT2780-1EA20)
SIMATIC RTLS Locating Manager (6GT2780-1EA30)
SIMATIC S7
SIMATIC S7-PLCSIM V17
SIMATIC STEP 7 V17
SIMATIC STEP 7 V18
SIMATIC STEP 7 V19

SIMATIC STEP 7 V20
SIMATIC STEP 7 V5
SIMATIC Target
SIMATIC WinCC
SIMATIC WinCC OA V3.19
SIMATIC WinCC OA V3.20
SIMATIC WinCC OA V3.21
SIMATIC WinCC Runtime Advanced V17
SIMATIC WinCC Unified PC Runtime V16
SIMATIC WinCC Unified PC Runtime V17
SIMATIC WinCC Unified PC Runtime V18
SIMATIC WinCC Unified PC Runtime V19
SIMATIC WinCC Unified PC Runtime V20
SIMATIC WinCC Unified PC Runtime V21
SIMATIC WinCC Unified Sequence
SIMATIC WinCC V17

SIMATIC WinCC V18
SIMATIC WinCC V19
SIMATIC WinCC V20
SIMATIC WinCC V7.5
SIMATIC WinCC V8.0
SIMATIC WinCC V8.1
SIMATIC eaSie Core Package (6DL5424-0AX00-0AV8)
SIMATIC eaSie PCS 7 Skill Package (6DL5424-0BX00-0AV8)
SIMOCODE ES V17
SIMOCODE ES V18
SIMOCODE ES V19
SIMOCODE ES V20
SIMOTION OACAMGEN (6AU1820-3EA20-0AB0)
SIMOTION SCOUT TIA V5.4
SIMOTION SCOUT TIA V5.5
SIMOTION SCOUT TIA V5.6

SIMOTION SCOUT TIA V5.7
SIMOVE Fleetmanager V3.1
SIMOVE Fleetmanager V3.2
SIMOVE Fleetmanager V3.3
SINAMICS G200
SINAMICS G220
SINAMICS S200
SINAMICS S210
SINAMICS S220
SINAMICS Startdrive
SINAMICS Startdrive V17
SINAMICS Startdrive V18
SINAMICS Startdrive V19
SINAMICS Startdrive V20
SINEC INS
SINEC NMS

SINEC Security Monitor
SINUMERIK Access MyMachine /OPC UA
SIPLANT
SIPROTEC 5 6MD84 (CP300)
SIPROTEC 5 6MD85 (CP200)
SIPROTEC 5 6MD85 (CP300)
SIPROTEC 5 6MD86 (CP200)
SIPROTEC 5 6MD86 (CP300)
SIPROTEC 5 6MD89 (CP300)
SIPROTEC 5 6MU85 (CP300)
SIPROTEC 5 7KE85 (CP200)
SIPROTEC 5 7KE85 (CP300)
SIPROTEC 5 7SA82 (CP100)
SIPROTEC 5 7SA82 (CP150)
SIPROTEC 5 7SA86 (CP200)
SIPROTEC 5 7SA86 (CP300)

SIPROTEC 5 7SA87 (CP200)
SIPROTEC 5 7SA87 (CP300)
SIPROTEC 5 7SD82 (CP100)
SIPROTEC 5 7SD82 (CP150)
SIPROTEC 5 7SD86 (CP200)
SIPROTEC 5 7SD86 (CP300)
SIPROTEC 5 7SD87 (CP200)
SIPROTEC 5 7SD87 (CP300)
SIPROTEC 5 7SJ81 (CP100)
SIPROTEC 5 7SJ81 (CP150)
SIPROTEC 5 7SJ82 (CP100)
SIPROTEC 5 7SJ82 (CP150)
SIPROTEC 5 7SJ85 (CP200)
SIPROTEC 5 7SJ85 (CP300)
SIPROTEC 5 7SJ86 (CP200)
SIPROTEC 5 7SJ86 (CP300)

SIPROTEC 5 7SK82 (CP100)
SIPROTEC 5 7SK82 (CP150)
SIPROTEC 5 7SK85 (CP200)
SIPROTEC 5 7SK85 (CP300)
SIPROTEC 5 7SL82 (CP100)
SIPROTEC 5 7SL82 (CP150)
SIPROTEC 5 7SL86 (CP200)
SIPROTEC 5 7SL86 (CP300)
SIPROTEC 5 7SL87 (CP200)
SIPROTEC 5 7SL87 (CP300)
SIPROTEC 5 7SS85 (CP200)
SIPROTEC 5 7SS85 (CP300)
SIPROTEC 5 7ST85 (CP200)
SIPROTEC 5 7ST85 (CP300)
SIPROTEC 5 7ST86 (CP300)
SIPROTEC 5 7SX82 (CP150)

SIPROTEC 5 7SX85 (CP300)
SIPROTEC 5 7SY82 (CP150)
SIPROTEC 5 7UM85 (CP300)
SIPROTEC 5 7UT82 (CP100)
SIPROTEC 5 7UT82 (CP150)
SIPROTEC 5 7UT85 (CP200)
SIPROTEC 5 7UT85 (CP300)
SIPROTEC 5 7UT86 (CP200)
SIPROTEC 5 7UT86 (CP300)
SIPROTEC 5 7UT87 (CP200)
SIPROTEC 5 7UT87 (CP300)
SIPROTEC 5 7VE85 (CP300)
SIPROTEC 5 7VK87 (CP200)
SIPROTEC 5 7VK87 (CP300)
SIPROTEC 5 7VU85 (CP300)
SIPROTEC 5 Compact 7SX800 (CP050)

SIRIUS Safety ES V17 (TIA Portal)
SIRIUS Safety ES V18 (TIA Portal)
SIRIUS Safety ES V19 (TIA Portal)
SIRIUS Safety ES V20 (TIA Portal)
SIRIUS Soft Starter ES V17 (TIA Portal)
SIRIUS Soft Starter ES V18 (TIA Portal)
SIRIUS Soft Starter ES V19 (TIA Portal)
SIRIUS Soft Starter ES V20 (TIA Portal)
SITRANS ASM IQ
SITRANS Soft Sensor Engine IQ (SITRANS SSE IQ)
Shopfloor IT Suite
Siemens OPC UA Modelling Editor (SiOME)
Simatic Step 7
TIA Portal Cloud V17
TIA Portal Cloud V18
TIA Portal Cloud V19

TIA Portal Cloud V20
TIA Portal Test Suite V20
User Management Component (UMC)
Visual Inspection Cockpit
simatic_pcs_neo_v5.0
simatic_pcs_neo_v6.0
simatic_step_7_v17
simatic_step_7_v19
simatic_step_7_v20
simatic_wincc_v18
simatic_wincc_v19
simatic_wincc_v20
simocode_es_v18
simotion_scout_tia_v5.4
simotion_scout_tia_v5.5
simotion_scout_tia_v5.6
simotion_scout_tia_v5.7
sinamics_startdrive_v17
sinamics_startdrive_v19
sinamics_startdrive_v20
sirius_safety_es_v18
sirius_safety_es_v19
sirius_safety_es_v20

sirius_soft_starter_es_v17
sirius_soft_starter_es_v18
sirius_soft_starter_es_v19
sirius_soft_starter_es_v20
tia_portal_cloud_v17
tia_portal_cloud_v18
tia_portal_cloud_v19
tia_portal_cloud_v20
tia_portal_test_suite_v20

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.