



# NCSC-2026-0229

## Kwetsbaarheden verholpen in Siemens producten

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 14-07-2026

**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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto:info@ncsc.nl)

## Feiten

Siemens heeft kwetsbaarheden verholpen in diverse producten als CADRA, IAM, Mendix, OpCenter, RUGGEDCOM, SIDIS en SIMATIC.

## 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
- Manipulatie van gegevens
- Omzeilen van een beveiligingsmaatregel
- (Remote) code execution (SYSTEM rechten)
- (Remote) code execution (Gebruikersrechten)
- 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-096828.html>
- <https://cert-portal.siemens.com/productcert/html/ssa-104023.html>
- <https://cert-portal.siemens.com/productcert/html/ssa-288252.html>
- <https://cert-portal.siemens.com/productcert/html/ssa-470355.html>
- <https://cert-portal.siemens.com/productcert/html/ssa-585531.html>
- <https://cert-portal.siemens.com/productcert/html/ssa-814963.html>
- <https://cert-portal.siemens.com/productcert/html/ssa-828211.html>

Kwetsbaarheden

| CVE              | CVSS Score   |
|------------------|--------------|
| > CVE-2005-2096  | 7.3 HIGH     |
| > CVE-2016-9840  | 8.8 HIGH     |
| > CVE-2016-9841  | 9.8 CRITICAL |
| > CVE-2016-9842  | 8.8 HIGH     |
| > CVE-2017-14919 | 7.5 HIGH     |
| > CVE-2018-25032 | 8.2 HIGH     |
| > CVE-2019-9494  | 5.9 MEDIUM   |
| > CVE-2019-9495  | 3.7 LOW      |
| > CVE-2022-23303 | 9.8 CRITICAL |
| > CVE-2022-23304 | 9.8 CRITICAL |
| > CVE-2022-37434 | 9.8 CRITICAL |
| > CVE-2022-37660 | 5.1 MEDIUM   |
| > CVE-2022-48174 | 9.8 CRITICAL |
| > CVE-2023-45853 | 9.8 CRITICAL |
| > CVE-2025-5222  | 5.1 MEDIUM   |
| > CVE-2025-5914  | 6.9 MEDIUM   |
| > CVE-2025-9230  | 6.9 MEDIUM   |
| > CVE-2025-9231  | 6.3 MEDIUM   |
| > CVE-2025-9232  | 6.3 MEDIUM   |
| > CVE-2025-10585 | 6.1 MEDIUM   |
| > CVE-2025-13223 | 6.1 MEDIUM   |

|                  |               |
|------------------|---------------|
| > CVE-2025-26465 | 6.3 MEDIUM    |
| > CVE-2025-32462 | 7.3 HIGH      |
| > CVE-2025-40945 | 8.5 HIGH      |
| > CVE-2026-0266  | 1.1 LOW       |
| > CVE-2026-0272  | 6.0 MEDIUM    |
| > CVE-2026-0273  | 6.1 MEDIUM    |
| > CVE-2026-5121  | 5.3 MEDIUM    |
| > CVE-2026-7891  | 9.1 CRITICAL  |
| > CVE-2026-22184 | 4.6 MEDIUM    |
| > CVE-2026-54429 | 6.0 MEDIUM    |
| > CVE-2026-56451 | 10.0 CRITICAL |

CWE's

| CWE       | Beschrijving                                                                               |
|-----------|--------------------------------------------------------------------------------------------|
| > CWE-20  | Improper Input Validation                                                                  |
| > 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-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-190 | Integer Overflow or Wraparound                                                             |

|            |                                                                                          |
|------------|------------------------------------------------------------------------------------------|
| ➤ CWE-203  | Observable Discrepancy                                                                   |
| ➤ CWE-208  | Observable Timing Discrepancy                                                            |
| ➤ CWE-277  | Insecure Inherited Permissions                                                           |
| ➤ CWE-294  | Authentication Bypass by Capture-replay                                                  |
| ➤ CWE-310  | Cryptographic Issues                                                                     |
| ➤ CWE-323  | Reusing a Nonce, Key Pair in Encryption                                                  |
| ➤ CWE-347  | Improper Verification of Cryptographic Signature                                         |
| ➤ CWE-385  | Covert Timing Channel                                                                    |
| ➤ CWE-390  | Detection of Error Condition Without Action                                              |
| ➤ CWE-415  | Double Free                                                                              |
| ➤ CWE-426  | Untrusted Search Path                                                                    |
| ➤ CWE-524  | Use of Cache Containing Sensitive Information                                            |
| ➤ CWE-680  | Integer Overflow to Buffer Overflow                                                      |
| ➤ CWE-770  | Allocation of Resources Without Limits or Throttling                                     |
| ➤ CWE-787  | Out-of-bounds Write                                                                      |
| ➤ CWE-843  | Access of Resource Using Incompatible Type ('Type Confusion')                            |
| ➤ CWE-862  | Missing Authorization                                                                    |
| ➤ CWE-863  | Incorrect Authorization                                                                  |
| ➤ CWE-924  | Improper Enforcement of Message Integrity During Transmission in a Communication Channel |
| ➤ CWE-1335 | Incorrect Bitwise Shift of Integer                                                       |

## Getroffen producten

### Siemens

CADRA

|                                                      |
|------------------------------------------------------|
| COMOS<br>V10.4.5                                     |
| COMOS<br>V10.6                                       |
| Cpu 1518F-4 Pn/Dp Mfp<br>Firmware                    |
| Designcenter<br>NX                                   |
| Mendix<br>Runtime                                    |
| Opcenter<br>X                                        |
| RUGGEDCOM<br>APE1808                                 |
| RUGGEDCOM RM1224 LTE(4G) EU<br>(6GK6108-4AM00-2BA2)  |
| RUGGEDCOM RM1224 LTE(4G) NAM<br>(6GK6108-4AM00-2DA2) |
| RUGGEDCOM ROX<br>MX5000                              |
| RUGGEDCOM ROX MX5000<br>FIRMWARE                     |
| RUGGEDCOM ROX<br>MX5000RE                            |
| RUGGEDCOM ROX<br>RX1400                              |
| RUGGEDCOM ROX RX1400<br>FIRMWARE                     |
| RUGGEDCOM ROX<br>RX1500                              |
| RUGGEDCOM ROX RX1500<br>FIRMWARE                     |

|                                       |
|---------------------------------------|
| RUGGEDCOM ROX<br>RX1501               |
| RUGGEDCOM ROX<br>RX1510               |
| RUGGEDCOM ROX RX1510<br>FIRMWARE      |
| RUGGEDCOM ROX<br>RX1511               |
| RUGGEDCOM ROX RX1511<br>FIRMWARE      |
| RUGGEDCOM ROX<br>RX1512               |
| RUGGEDCOM ROX RX1512<br>FIRMWARE      |
| RUGGEDCOM ROX<br>RX1524               |
| RUGGEDCOM ROX RX1524<br>Firmware      |
| RUGGEDCOM ROX<br>RX1536               |
| RUGGEDCOM ROX RX1536<br>Firmware      |
| RUGGEDCOM ROX<br>RX5000               |
| RUGGEDCOM<br>RST2428P                 |
| RUGGEDCOM RST2428P<br>(6GK6242-6PA00) |
| Ruggedcom Rox Mx5000Re<br>Firmware    |
| Ruggedcom Rox Rx1501<br>Firmware      |

|                                                               |
|---------------------------------------------------------------|
| Ruggedcom Rox Rx5000<br>Firmware                              |
| SCALANCE M804PB<br>(6GK5804-0AP00-2AA2)                       |
| SCALANCE M812-1 ADSL-Router (Annex A)<br>(6GK5812-1AA00-2AA2) |
| SCALANCE M812-1 ADSL-Router (Annex B)<br>(6GK5812-1BA00-2AA2) |
| SCALANCE M816-1 ADSL-Router (Annex A)<br>(6GK5816-1AA00-2AA2) |
| SCALANCE M816-1 ADSL-Router (Annex B)<br>(6GK5816-1BA00-2AA2) |
| SCALANCE M826-2 SHDSL-Router<br>(6GK5826-2AB00-2AB2)          |
| SCALANCE M874-2<br>(6GK5874-2AA00-2AA2)                       |
| SCALANCE M874-3<br>(6GK5874-3AA00-2AA2)                       |
| SCALANCE M876-3 (EVDO)<br>(6GK5876-3AA02-2BA2)                |
| SCALANCE M876-3 (ROK)<br>(6GK5876-3AA02-2EA2)                 |
| SCALANCE M876-4<br>(6GK5876-4AA10-2BA2)                       |
| SCALANCE M876-4 (EU)<br>(6GK5876-4AA00-2BA2)                  |
| SCALANCE M876-4 (NAM)<br>(6GK5876-4AA00-2DA2)                 |
| SCALANCE MUM853-1 (EU)<br>(6GK5853-2EA00-2DA1)                |
| SCALANCE MUM856-1 (EU)<br>(6GK5856-2EA00-3DA1)                |

|                                                 |
|-------------------------------------------------|
| SCALANCE MUM856-1 (RoW)<br>(6GK5856-2EA00-3AA1) |
| SCALANCE S615<br>(6GK5615-0AA00-2AA2)           |
| SCALANCE S615 EEC<br>(6GK5615-0AA01-2AA2)       |
| SCALANCE S615<br>Firmware                       |
| SCALANCE SC622-2C<br>(6GK5622-2GS00-2AC2)       |
| SCALANCE SC622-2C<br>Firmware                   |
| SCALANCE SC626-2C<br>(6GK5626-2GS00-2AC2)       |
| SCALANCE SC626-2C<br>Firmware                   |
| SCALANCE<br>SC632-2C                            |
| SCALANCE SC632-2C<br>(6GK5632-2GS00-2AC2)       |
| SCALANCE SC632-2C<br>Firmware                   |
| SCALANCE SC636-2C<br>(6GK5636-2GS00-2AC2)       |
| SCALANCE SC636-2C<br>Firmware                   |
| SCALANCE SC642-2C<br>(6GK5642-2GS00-2AC2)       |
| SCALANCE SC642-2C<br>Firmware                   |
| SCALANCE<br>SC646-2C                            |

|                                                          |
|----------------------------------------------------------|
| SCALANCE SC646-2C<br>(6GK5646-2GS00-2AC2)                |
| SCALANCE SC646-2C<br>Firmware                            |
| SCALANCE WAM763-1<br>(6GK5763-1AL00-7DA0)                |
| SCALANCE WAM766-1 (EU)<br>(6GK5766-1GE00-7DA0)           |
| SCALANCE WAM766-1 (US)<br>(6GK5766-1GE00-7DB0)           |
| SCALANCE WAM766-1 EEC (EU)<br>(6GK5766-1GE00-7TA0)       |
| SCALANCE WAM766-1 EEC (US)<br>(6GK5766-1GE00-7TB0)       |
| SCALANCE<br>WUM763-1                                     |
| SCALANCE WUM763-1<br>(6GK5763-1AL00-3AA0)                |
| SCALANCE WUM763-1<br>(6GK5763-1AL00-3DA0)                |
| SCALANCE WUM766-1 (EU)<br>(6GK5766-1GE00-3DA0)           |
| SCALANCE WUM766-1 (US)<br>(6GK5766-1GE00-3DB0)           |
| SCALANCE XC-300/XR-300/XC-400/<br>XR-500WG/XR-500 family |
| SCALANCE<br>XCH328                                       |
| SCALANCE XCH328<br>(6GK5328-4TS01-2EC2)                  |
| SCALANCE<br>XCM324                                       |

|                                                                          |
|--------------------------------------------------------------------------|
| SCALANCE XCM324<br>(6GK5324-8TS01-2AC2)                                  |
| SCALANCE<br>XCM328                                                       |
| SCALANCE XCM328<br>(6GK5328-4TS01-2AC2)                                  |
| SCALANCE<br>XCM332                                                       |
| SCALANCE XCM332<br>(6GK5332-0GA01-2AC2)                                  |
| SCALANCE XRH334 (24 V DC,<br>8xFO, CC)                                   |
| SCALANCE XRH334 (24 V DC, 8xFO, CC)<br>(6GK5334-2TS01-2ER3)              |
| SCALANCE XRM334 (230 V<br>AC, 12xFO)                                     |
| SCALANCE XRM334 (230 V AC, 12xFO)<br>(6GK5334-3TS01-3AR3)                |
| SCALANCE XRM334 (230 V<br>AC, 8xFO)                                      |
| SCALANCE XRM334 (230 V AC, 8xFO)<br>(6GK5334-2TS01-3AR3)                 |
| SCALANCE XRM334 (230V AC,<br>2x10G, 24xSFP, 8xSFP+)                      |
| SCALANCE XRM334 (230V AC, 2x10G, 24xSFP,<br>8xSFP+) (6GK5334-5TS01-3AR3) |
| SCALANCE XRM334 (24 V<br>DC, 12xFO)                                      |
| SCALANCE XRM334 (24 V DC, 12xFO)<br>(6GK5334-3TS01-2AR3)                 |
| SCALANCE XRM334 (24 V<br>DC, 8xFO)                                       |

|                                                                            |
|----------------------------------------------------------------------------|
| SCALANCE XRM334 (24 V DC, 8xFO)<br>(6GK5334-2TS01-2AR3)                    |
| SCALANCE XRM334 (24V DC, 2x10G,<br>24xSFP, 8xSFP+)                         |
| SCALANCE XRM334 (24V DC, 2x10G, 24xSFP,<br>8xSFP+) (6GK5334-5TS01-2AR3)    |
| SCALANCE XRM334 (2x230 V<br>AC, 12xFO)                                     |
| SCALANCE XRM334 (2x230 V AC, 12xFO)<br>(6GK5334-3TS01-4AR3)                |
| SCALANCE XRM334 (2x230 V<br>AC, 8xFO)                                      |
| SCALANCE XRM334 (2x230 V AC, 8xFO)<br>(6GK5334-2TS01-4AR3)                 |
| SCALANCE XRM334 (2x230V AC,<br>2x10G, 24xSFP, 8xSFP+)                      |
| SCALANCE XRM334 (2x230V AC, 2x10G, 24xSFP,<br>8xSFP+) (6GK5334-5TS01-4AR3) |
| SIDIS<br>Prime                                                             |
| SIDIS Secured<br>SmartPlug                                                 |
| SIMATIC CN<br>4100                                                         |
| SIMATIC MV540 H<br>(6GF3540-0GE10)                                         |
| SIMATIC MV540 H<br>Firmware                                                |
| SIMATIC MV540 S<br>(6GF3540-0CD10)                                         |
| SIMATIC MV540 S<br>Firmware                                                |

|                                                               |
|---------------------------------------------------------------|
| SIMATIC MV550 H<br>(6GF3550-0GE10)                            |
| SIMATIC MV550 H<br>Firmware                                   |
| SIMATIC MV550 S<br>(6GF3550-0CD10)                            |
| SIMATIC MV560 U<br>(6GF3560-0LE10)                            |
| SIMATIC MV560 U<br>Firmware                                   |
| SIMATIC MV560 X<br>(6GF3560-0HE10)                            |
| SIMATIC MV560 X<br>Firmware                                   |
| SIMATIC<br>S7                                                 |
| SIMATIC S7 CPU 1500<br>firmware                               |
| SIMATIC<br>S7-1500                                            |
| SIMATIC S7-1500 CPU 1518-4<br>PN/DP MFP                       |
| SIMATIC S7-1500 CPU 1518-4 PN/DP MFP<br>(6ES7518-4AX00-1AB0)  |
| SIMATIC S7-1500 CPU 1518-4 PN/DP MFP<br>(6ES7518-4AX00-1AC0)  |
| SIMATIC S7-1500 CPU 1518-4 PN/<br>DP MFP Firmware             |
| SIMATIC S7-1500 CPU 1518F-4<br>PN/DP MFP                      |
| SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP<br>(6ES7518-4FX00-1AB0) |

|                                                               |
|---------------------------------------------------------------|
| SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP<br>(6ES7518-4FX00-1AC0) |
| SIMATIC S7-1500 TM MFP - GNU/<br>Linux subsystem              |
| SIMATIC S7-PLCSIM<br>Advanced                                 |
| SINAMICS PERFECT HARMONY<br>GH180 6SR5                        |
| SINEC<br>PNI                                                  |
| SIPLUS S7-1500 CPU 1518-4<br>PN/DP MFP                        |
| SIPLUS S7-1500 CPU 1518-4 PN/DP MFP<br>(6AG1518-4AX00-4AC0)   |
| Scalance Sc622-2C<br>Firmware                                 |
| Scalance Sc632-2C<br>Firmware                                 |
| Scalance Sc646-2C<br>Firmware                                 |
| Scalance W700 IEEE 802.11Ax<br>Firmware                       |
| Scalance<br>Wam763-1                                          |
| Scalance<br>Wam766-1                                          |
| Scalance<br>Wam766-1 Eec                                      |
| Scalance<br>Wum766-1                                          |
| Simatic Mv550 S<br>Firmware                                   |

|                                            |
|--------------------------------------------|
| Simcenter<br>3D                            |
| Simcenter Femap<br>V2506                   |
| Simcenter Femap<br>V2512                   |
| Simcenter<br>Nastran                       |
| Simcenter STAR-<br>CCM+                    |
| Sinamics Perfect Harmony<br>Gh180 Firmware |
| Sinec<br>Pni                               |
| Solid Edge<br>SE2025                       |
| Solid Edge<br>SE2026                       |
| Teamcenter Visualization<br>V2412          |
| Teamcenter Visualization<br>V2506          |
| Teamcenter Visualization<br>V2512          |
| Tecnomatix Plant<br>Simulation V2404       |
| Tecnomatix Plant<br>Simulation V2504       |
| Tecnomatix Process<br>Simulate             |
| scalance_sc622-2c                          |
| scalance_sc626-2c                          |

|                            |
|----------------------------|
| scalance_sc626-2c_firmware |
| scalance_sc636-2c          |
| scalance_sc636-2c_firmware |
| scalance_sc642-2c          |
| scalance_sc642-2c_firmware |

## 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.