Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0357

Kwetsbaarheden verholpen in Siemens producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 11-11-2025

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 Altair Grid Engine, COMOS, LOGO, SICAM, SIDOOR, SIMATIC, SIPLUS, Spectrum Power 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-201498.html
- https://cert-portal.siemens.com/productcert/html/ssa-267056.html
- https://cert-portal.siemens.com/productcert/html/ssa-339694.html
- https://cert-portal.siemens.com/productcert/html/ssa-514895.html
- https://cert-portal.siemens.com/productcert/html/ssa-522291.html
- https://cert-portal.siemens.com/productcert/html/ssa-682326.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2023-30901	8.8 HIGH
CVE-2023-31238	5.5 MEDIUM
CVE-2023-45133	9.3 CRITICAL
CVE-2024-0056	8.7 HIGH
CVE-2024-32008	7.8 HIGH
CVE-2024-32009	7.8 HIGH
CVE-2024-32010	7.8 HIGH
CVE-2024-32011	8.8 HIGH
CVE-2024-32014	4.7 MEDIUM
CVE-2025-2884	6.6 MEDIUM
CVE-2025-40744	7.5 HIGH
CVE-2025-40760	5.5 MEDIUM
CVE-2025-40763	7.8 HIGH
CVE-2025-40815	7.2 HIGH
CVE-2025-40816	7.6 HIGH
CVE-2025-40817	6.5 MEDIUM
CVE-2025-40827	7.8 HIGH

CWE's

CWE	Beschrijving
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

CWE-125	Out-of-bounds Read
CWE-184	Incomplete List of Disallowed Inputs
CWE-209	Generation of Error Message Containing Sensitive Information
CWE-266	Incorrect Privilege Assignment
CWE-295	Improper Certificate Validation
CWE-306	Missing Authentication for Critical Function
CWE-319	Cleartext Transmission of Sensitive Information
CWE-352	Cross-Site Request Forgery (CSRF)
CWE-420	Unprotected Alternate Channel
CWE-427	Uncontrolled Search Path Element
CWE-648	Incorrect Use of Privileged APIs
CWE-697	Incorrect Comparison
CWE-732	Incorrect Permission Assignment for Critical Resource
CWE-829	Inclusion of Functionality from Untrusted Control Sphere

Getroffen producten

Siemens
Altair Grid Engine
COMOS
INTRALOG WMS
JT2Go (Application)
LOGO! 12/24RCE (6ED1052-1MD08-0BA2)

LOGO! 12/24RCEo (6ED1052-2MD08-0BA2)
LOGO! 230RCE (6ED1052-1FB08-0BA2)
LOGO! 230RCEo (6ED1052-2FB08-0BA2)
LOGO! 24CE (6ED1052-1CC08-0BA2)
LOGO! 24CEo (6ED1052-2CC08-0BA2)
LOGO! 24RCE (6ED1052-1HB08-0BA2)
LOGO! 24RCEo (6ED1052-2HB08-0BA2)
POWER METER SICAM Q100
POWER METER SICAM Q100 (7KG9501-0AA01-0AA1)
POWER METER SICAM Q100 (7KG9501-0AA01-2AA1)
POWER METER SICAM Q100 (7KG9501-0AA31-0AA1)
POWER METER SICAM Q100 (7KG9501-0AA31-2AA1)
POWER METER SICAM Q200 family
Power Meter Sicam Q100
Power Meter Sicam Q200 Firmware
Q200 Firmware
SICAM

SICAM P850 (7KG8500-0AA00-0AA0)
SICAM P850 (7KG8500-0AA00-2AA0)
SICAM P850 (7KG8500-0AA10-0AA0)
SICAM P850 (7KG8500-0AA10-2AA0)
SICAM P850 (7KG8500-0AA30-0AA0)
SICAM P850 (7KG8500-0AA30-2AA0)
SICAM P850 (7KG8501-0AA01-0AA0)
SICAM P850 (7KG8501-0AA01-2AA0)
SICAM P850 (7KG8501-0AA02-0AA0)
SICAM P850 (7KG8501-0AA02-2AA0)
SICAM P850 (7KG8501-0AA11-0AA0)
SICAM P850 (7KG8501-0AA11-2AA0)
SICAM P850 (7KG8501-0AA12-0AA0)
SICAM P850 (7KG8501-0AA12-2AA0)
SICAM P850 (7KG8501-0AA31-0AA0)
SICAM P850 (7KG8501-0AA31-2AA0)

SICAM P850 (7KG8501-0AA32-0AA0)
SICAM P850 (7KG8501-0AA32-2AA0)
SICAM P850 Firmware (OS)
SICAM P855 (7KG8550-0AA00-0AA0)
SICAM P855 (7KG8550-0AA00-2AA0)
SICAM P855 (7KG8550-0AA10-0AA0)
SICAM P855 (7KG8550-0AA10-2AA0)
SICAM P855 (7KG8550-0AA30-0AA0)
SICAM P855 (7KG8550-0AA30-2AA0)
SICAM P855 (7KG8551-0AA01-0AA0)
SICAM P855 (7KG8551-0AA01-2AA0)
SICAM P855 (7KG8551-0AA02-0AA0)
SICAM P855 (7KG8551-0AA02-2AA0)
SICAM P855 (7KG8551-0AA11-0AA0)
SICAM P855 (7KG8551-0AA11-2AA0)
SICAM P855 (7KG8551-0AA12-0AA0)

SICAM P855 (7KG8551-0AA12-2AA0)
SICAM P855 (7KG8551-0AA31-0AA0)
SICAM P855 (7KG8551-0AA31-2AA0)
SICAM P855 (7KG8551-0AA32-0AA0)
SICAM P855 (7KG8551-0AA32-2AA0)
SICAM P855 Firmware (OS)
SIDIS Prime
SIPLUS LOGO! 12/24RCE (6AG1052-1MD08-7BA2)
SIPLUS LOGO! 12/24RCEo (6AG1052-2MD08-7BA2)
SIPLUS LOGO! 230RCE (6AG1052-1FB08-7BA2)
SIPLUS LOGO! 230RCEo (6AG1052-2FB08-7BA2)
SIPLUS LOGO! 24CE (6AG1052-1CC08-7BA2)
SIPLUS LOGO! 24CEo (6AG1052-2CC08-7BA2)
SIPLUS LOGO! 24RCE (6AG1052-1HB08-7BA2)
SIPLUS LOGO! 24RCEo (6AG1052-2HB08-7BA2)
Sidis Prime

Siemens SICAM
Siemens Software Center
Siveillance Video
Siveillance Video 2022 R1
Siveillance Video 2022 R2
Siveillance Video 2022 R3
Siveillance Video 2023 R1
Siveillance Video 2023 R2
Siveillance Video 2023 R3
Solid Edge SE2025
Spectrum Power 4
Teamcenter Visualization
q200_firmware
Power Meter Sicam Q200 Family

Disclaimer