Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0473

Kwetsbaarheden verholpen in Siemens producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 10-12-2024

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 COMOS, RUGGEDCOM, SENTRON, SICAM, SIMATIC 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)
- Manipulatie van gegevens
- Omzeilen van een beveiligingsmaatregel
- Omzeilen van authenticatie
- (Remote) code execution (Administrator/Root rechten)
- (Remote) code execution (Gebruikersrechten)
- Toegang tot systeemgegevens
- Verhoogde gebruikersrechten

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-128393.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-384652.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-392859.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-620799.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-645131.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-701627.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-730188.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-800126.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-881356.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-979056.pdf

Kwetsbaarheden

CVE	CVSS Score
CVE-2020-28398	8.8 HIGH
CVE-2024-6657	6.5 MEDIUM
CVE-2024-41981	
CVE-2024-45463	
CVE-2024-45464	7.8 HIGH
CVE-2024-45465	7.8 HIGH
CVE-2024-45466	7.8 HIGH
CVE-2024-45467	
CVE-2024-45468	
CVE-2024-45469	
CVE-2024-45470	7.8 HIGH
CVE-2024-45471	
CVE-2024-45472	
CVE-2024-45473	7.8 HIGH
CVE-2024-45474	
CVE-2024-45475	
CVE-2024-45476	3.3 LOW
CVE-2024-47046	7.8 HIGH
CVE-2024-49704	
CVE-2024-49849	
CVE-2024-52051	

CVE-2024-52565	7.8 HIGH
CVE-2024-52566	7.8 HIGH
CVE-2024-52567	7.8 HIGH
CVE-2024-52568	7.8 HIGH
CVE-2024-52569	7.8 HIGH
CVE-2024-52570	7.8 HIGH
CVE-2024-52571	7.8 HIGH
CVE-2024-52572	7.8 HIGH
CVE-2024-52573	7.8 HIGH
CVE-2024-52574	7.8 HIGH
CVE-2024-53041	
CVE-2024-53242	
CVE-2024-53832	4.6 MEDIUM
CVE-2024-54005	
CVE-2024-54093	
CVE-2024-54094	
CVE-2024-54095	7.8 HIGH

CWE's

CWE	Beschrijving
CWE-191	Integer Underflow (Wrap or Wraparound)
CWE-522	Insufficiently Protected Credentials
CWE-125	Out-of-bounds Read
CWE-352	Cross-Site Request Forgery (CSRF)

CWE-502	Deserialization of Untrusted Data
CWE-611	Improper Restriction of XML External Entity Reference
CWE-122	Heap-based Buffer Overflow
CWE-121	Stack-based Buffer Overflow
CWE-20	Improper Input Validation

Getroffen producten

siemens
comos
comos_v10.3
comos_v10.4.0
comos_v10.4.1
comos_v10.4.2
comos_v10.4.3
comos_v10.4.4.1
comos_v10.4.4
cpci85_central_processing_communication
ruggedcom_rox_mx5000
ruggedcom_rox_mx5000re
ruggedcom_rox_rx1400
ruggedcom_rox_rx1500
ruggedcom_rox_rx1501
ruggedcom_rox_rx1510
ruggedcom_rox_rx1511
ruggedcom_rox_rx1512

ruggedcom_rox_rx1524
ruggedcom_rox_rx1536
ruggedcom_rox_rx5000
sentron_powercenter_1000__7kn1110-0mc00_
sentron_powercenter_1100__7kn1111-0mc00_
simatic_s7- plcsim
simatic_s7- plcsim_v16
simatic_s7- plcsim_v17
simatic_s7- plcsim_v18
simatic_step_7
simatic_step_7_safety
simatic_step_7_safety_v16
simatic_step_7_safety_v17
simatic_step_7_safety_v18
simatic_step_7_safety_v19
simatic_step_7_v16
simatic_step_7_v17
simatic_step_7_v18
simatic_step_7_v19
simatic_wincc
simatic_wincc_unified
simatic_wincc_unified_pc_runtime_v18
simatic_wincc_unified_pc_runtime_v19

simatic_wincc_unified_v16
simatic_wincc_unified_v17
simatic_wincc_unified_v18
simatic_wincc_unified_v19
simatic_wincc_v16
simatic_wincc_v17
simatic_wincc_v18
simatic_wincc_v19
simcenter_femap_v2306
simcenter_femap_v2401
simcenter_femap_v2406
simcenter_nastran
simcenter_nastran_2306
simcenter_nastran_2312
simcenter_nastran_2406
simocode_es
simocode_es_v16
simocode_es_v17
simocode_es_v18
simocode_es_v19
simotion_scout_tia
simotion_scout_tia_v5.4_sp1
simotion_scout_tia_v5.4_sp3
simotion_scout_tia_v5.5_sp1
simotion_scout_tia_v5.6_sp1
sinamics_startdrive

sinamics_startdrive_v16
sinamics_startdrive_v17
sinamics_startdrive_v18
sinamics_startdrive_v19
sirius_safety_es
sirius_safety_es_v17__tia_portal_
sirius_safety_es_v18__tia_portal_
sirius_safety_es_v19__tia_portal_
sirius_soft_starter_es_v17__tia_portal_
sirius_soft_starter_es_v18__tia_portal_
sirius_soft_starter_es_v19__tia_portal_
solid_edge_se2024
teamcenter_visualization
teamcenter_visualization_v14.2
teamcenter_visualization_v14.3
teamcenter_visualization_v2312
teamcenter_visualization_v2406
tecnomatix_plant_simulation
tecnomatix_plant_simulation_v2302
tecnomatix_plant_simulation_v2404
tia_portal_cloud
tia_portal_cloud_v16
tia_portal_cloud_v17
tia_portal_cloud_v18
tia_portal_cloud_v19

Disclaimer