Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0433

Kwetsbaarheden verholpen in Siemens producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 12-11-2024

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 Mendix, RUGGEDCOM, SCALANCE, SIMATIC en SINEC.

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-000297.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-064257.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-230445.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-331112.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-351178.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-354112.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-454789.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-616032.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-654798.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-871035.pdf

- https://cert-portal.siemens.com/productcert/pdf/ssa-914892.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-915275.pdf

Kwetsbaarheden

CVE	CVSS Score
CVE-2021-3506	
CVE-2023-2975	7.8 HIGH
CVE-2023-3341	
CVE-2023-3446	7.8 HIGH
CVE-2023-3817	7.8 HIGH
CVE-2023-4236	
CVE-2023-4408	
CVE-2023-4807	7.8 HIGH
CVE-2023-5363	7.5 HIGH
CVE-2023-5517	
CVE-2023-5678	
CVE-2023-5679	
CVE-2023-5680	
CVE-2023-6129	
CVE-2023-6237	
CVE-2023-6516	
CVE-2023-7104	7.3 HIGH
CVE-2023-28450	7.5 HIGH
CVE-2023-30584	9.1 CRITICAL

CVE-2023-32002	9.8 CRITICAL
CVE-2023-32003	
CVE-2023-32004	8.8 HIGH
CVE-2023-32005	
CVE-2023-32006	9.8 CRITICAL
CVE-2023-32558	7.5 HIGH
CVE-2023-32559	9.8 CRITICAL
CVE-2023-32736	7.3 HIGH
CVE-2023-38552	
CVE-2023-38709	
CVE-2023-39331	
CVE-2023-39332	
CVE-2023-39333	
CVE-2023-44487	7.5 HIGH
CVE-2023-45143	
CVE-2023-46218	6.5 MEDIUM
CVE-2023-46219	9.8 CRITICAL
CVE-2023-46280	6.5 MEDIUM
CVE-2023-46809	
CVE-2023-47038	
CVE-2023-47039	
CVE-2023-47100	
CVE-2023-48795	5.9 MEDIUM

CVE-2023-49441	
CVE-2023-50387	
CVE-2023-50868	
CVE-2023-52389	
CVE-2024-0232	
CVE-2024-0727	7.5 HIGH
CVE-2024-2004	5.3 MEDIUM
CVE-2024-2379	5.9 MEDIUM
CVE-2024-2398	8.6 HIGH
CVE-2024-2466	7.1 HIGH
CVE-2024-2511	7.5 HIGH
CVE-2024-4603	
CVE-2024-4741	
CVE-2024-5535	9.1 CRITICAL
CVE-2024-5594	
CVE-2024-21890	
CVE-2024-21891	
CVE-2024-21892	
CVE-2024-21896	
CVE-2024-22017	
CVE-2024-22019	
CVE-2024-22025	
CVE-2024-24758	

CVE-2024-24795	
CVE-2024-24806	
CVE-2024-26306	
CVE-2024-26925	
CVE-2024-27316	
CVE-2024-27980	
CVE-2024-27982	
CVE-2024-27983	
CVE-2024-28882	
CVE-2024-29119	7.8 HIGH
CVE-2024-36140	6.8 MEDIUM
CVE-2024-44102	10.0 CRITICAL
CVE-2024-46888	9.9 CRITICAL
CVE-2024-46889	5.3 MEDIUM
CVE-2024-46890	9.1 CRITICAL
CVE-2024-46891	5.3 MEDIUM
CVE-2024-46892	4.9 MEDIUM
CVE-2024-46894	6.3 MEDIUM
CVE-2024-47783	7.8 HIGH
CVE-2024-47808	8.4 HIGH
CVE-2024-47940	7.8 HIGH
CVE-2024-47941	7.8 HIGH
CVE-2024-47942	7.3 HIGH

CVE-2024-50310	7.5 HIGH
CVE-2024-50313	5.3 MEDIUM
CVE-2024-50557	7.2 HIGH
CVE-2024-50558	4.3 MEDIUM
CVE-2024-50559	4.3 MEDIUM
CVE-2024-50560	3.1 LOW
CVE-2024-50561	4.3 MEDIUM
CVE-2024-50572	7.2 HIGH

CWE's

CWE	Beschrijving
CWE-606	Unchecked Input for Loop Condition
CWE-1240	Use of a Cryptographic Primitive with a Risky Implementation
CWE-115	Misinterpretation of Input
CWE-1059	Insufficient Technical Documentation
CWE-1325	Improperly Controlled Sequential Memory Allocation
CWE-222	Truncation of Security-relevant Information
CWE-310	CWE-310
CWE-328	Use of Weak Hash
CWE-1284	Improper Validation of Specified Quantity in Input
CWE-213	Exposure of Sensitive Information Due to Incompatible Policies
CWE-1268	Policy Privileges are not Assigned Consistently Between Control and Data Agents
CWE-684	Incorrect Provision of Specified Functionality
CWE-772	Missing Release of Resource after Effective Lifetime

CWE-208	Observable Timing Discrepancy
CWE-201	Insertion of Sensitive Information Into Sent Data
CWE-834	Excessive Iteration
CWE-266	Incorrect Privilege Assignment
CWE-942	Permissive Cross-domain Policy with Untrusted Domains
CWE-271	Privilege Dropping / Lowering Errors
CWE-732	Incorrect Permission Assignment for Critical Resource
CWE-667	Improper Locking
CWE-440	Expected Behavior Violation
CWE-297	Improper Validation of Certificate with Host Mismatch
CWE-311	Missing Encryption of Sensitive Data
CWE-754	Improper Check for Unusual or Exceptional Conditions
CWE-617	Reachable Assertion
CWE-427	Uncontrolled Search Path Element
CWE-319	Cleartext Transmission of Sensitive Information
CWE-613	Insufficient Session Expiration
CWE-444	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')
CWE-203	Observable Discrepancy
CWE-354	Improper Validation of Integrity Check Value
CWE-325	Missing Cryptographic Step
CWE-190	Integer Overflow or Wraparound
CWE-321	Use of Hard-coded Cryptographic Key
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-125	Out-of-bounds Read
CWE-404	Improper Resource Shutdown or Release

CWE-275	CWE-275
CWE-284	Improper Access Control
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
CWE-1333	Inefficient Regular Expression Complexity
CWE-416	Use After Free
CWE-113	Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting')
CWE-401	Missing Release of Memory after Effective Lifetime
CWE-476	NULL Pointer Dereference
CWE-295	Improper Certificate Validation
CWE-757	Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade')
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-327	Use of a Broken or Risky Cryptographic Algorithm
CWE-436	Interpretation Conflict
CWE-400	Uncontrolled Resource Consumption
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')
CWE-502	Deserialization of Untrusted Data
CWE-918	Server-Side Request Forgery (SSRF)
CWE-863	Incorrect Authorization
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-787	Out-of-bounds Write
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor

CWE-122	Heap-based Buffer Overflow
CWE-121	Stack-based Buffer Overflow
CWE-789	Memory Allocation with Excessive Size Value
CWE-269	Improper Privilege Management
CWE-20	Improper Input Validation
CWE-287	Improper Authentication
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

siemens
mendix_runtime_v10.12
mendix_runtime_v10.6
mendix_runtime_v10
mendix_runtime_v8
mendix_runtime_v9
ozw672
ozw772
pp_telecontrol_server_basic_1000_to_5000_v3.1
pp_telecontrol_server_basic_256_to_1000_v3.1
pp_telecontrol_server_basic_32_to_64_v3.1
pp_telecontrol_server_basic_64_to_256_v3.1
pp_telecontrol_server_basic_8_to_32_v3.1
ruggedcom_ape1808
ruggedcom_rm1224_lte_4g__eu
ruggedcom_rm1224_lte_4g__nam

s7- pct
s7_port_configuration_tool
scalance_m804pb
scalance_m812-1_adsl- router
scalance_m816-1_adsl- router
scalance_m826-2_shdsl- router
scalance_m874-2
scalance_m874-3
scalance_m874-3_3g- router__cn_
scalance_m876-3
scalance_m876-3__rok_
scalance_m876-4
scalance_m876-4__eu_
scalance_m876-4__nam_
scalance_mum853-1__a1_
scalance_mum853-1__b1_
scalance_mum853-1__eu_
scalance_mum856-1__a1_
scalance_mum856-1__b1_
scalance_mum856-1__cn_
scalance_mum856-1__eu_
scalance_mum856-1__row_

scalance_s615_eec_lan- router
scalance_s615_lan- router
scalance_xch328__6gk5328-4ts01-2ec2_
scalance_xcm324__6gk5324-8ts01-2ac2_
scalance_xcm328__6gk5328-4ts01-2ac2_
scalance_xcm332__6gk5332-0ga01-2ac2_
scalance_xrh334__24_v_dc__8xfo__cc___6gk5334-2ts01-2er3_
scalance_xrm334__230_v_ac__12xfo___6gk5334-3ts01-3ar3_
scalance_xrm334__230_v_ac__8xfo___6gk5334-2ts01-3ar3_
scalance_xrm334__24_v_dc__12xfo___6gk5334-3ts01-2ar3_
scalance_xrm334__24_v_dc__8xfo___6gk5334-2ts01-2ar3_
scalance_xrm334__2x230_v_ac__12xfo___6gk5334-3ts01-4ar3_
scalance_xrm334__2x230_v_ac__8xfo___6gk5334-2ts01-4ar3_
security_configuration_tool
security_configuration_tool__sct_
simatic_automation_tool
simatic_batch_v9.1
simatic_cp_1543-1_v4.0
simatic_mv500_family
simatic_net_pc- software
simatic_net_pc_software
simatic_net_pc_software_v16
simatic_net_pc_software_v17
simatic_net_pc_software_v18

simatic_net_pc_software_v19
simatic_pcs
simatic_pcs_7_v9.1
simatic_pdm_v9.2
simatic_route_control_
simatic_route_control_v9.1
simatic_rtls_locating_manager
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_s7-1500_cpu_1518-4_pn_dp_mfp__6es7518-4ax00-1ab0_
simatic_s7-1500_cpu_1518-4_pn_dp_mfp__6es7518-4ax00-1ac0_
simatic_s7-1500_cpu_1518f-4_pn_dp_mfp__6es7518-4fx00-1ab0_
simatic_s7-1500_cpu_1518f-4_pn_dp_mfp__6es7518-4fx00-1ac0_
simatic_s7-1500_tm_mfp_- _gnu_linux_subsystem
simatic_s7- plcsim_v16
simatic_s7- plcsim_v17
simatic_step_7_safety_v16
simatic_step_7_safety_v17
simatic_step_7_safety_v18

simatic_step_7_v16
simatic_step_7_v17
simatic_step_7_v18
simatic_step_7_v5
simatic_wincc
simatic_wincc_oa_v3.17
simatic_wincc_oa_v3.18
simatic_wincc_oa_v3.19
simatic_wincc_runtime_advanced
simatic_wincc_runtime_professional
simatic_wincc_runtime_professional_v16
simatic_wincc_runtime_professional_v17
simatic_wincc_runtime_professional_v18
simatic_wincc_runtime_professional_v19
simatic_wincc_unified_pc_runtime
simatic_wincc_unified_pc_runtime_v18
simatic_wincc_unified_v16
simatic_wincc_unified_v17
simatic_wincc_unified_v18
simatic_wincc_v16
simatic_wincc_v17
simatic_wincc_v18
simatic_wincc_v7.4
simatic_wincc_v7.5
simatic_wincc_v8.0
simocode_es_v16

simocode_es_v17
simocode_es_v18
simotion_scout_tia_v5.4_sp1
simotion_scout_tia_v5.4_sp3
simotion_scout_tia_v5.5_sp1
sinamics_startdrive
sinamics_startdrive_v16
sinamics_startdrive_v17
sinamics_startdrive_v18
sinec_ins
sinec_network_management_system
sinec_nms
sinema_remote_connect_client
sinumerik_one_virtual
sinumerik_plc_programming_tool
siplus_s7-1500_cpu_1518-4_pn_dp_mfp__6ag1518-4ax00-4ac0_
siport
sirius_safety_es_v17
sirius_safety_es_v18
sirius_soft_starter_es_v17
sirius_soft_starter_es_v18
solid_edge_se2024
spectrum_power_7
st7_scadaconnect
st7_scadaconnect__6nh7997-5da10-0aa0_
telecontrol_server_basic

telecontrol_server_basic_1000_v3.1
telecontrol_server_basic_256_v3.1
telecontrol_server_basic_32_v3.1
telecontrol_server_basic_5000_v3.1
telecontrol_server_basic_64_v3.1
telecontrol_server_basic_8_v3.1
telecontrol_server_basic_serv_upgr
telecontrol_server_basic_upgr_v3.1
telecontrol_server_basic_v3
tia_portal_cloud_connector
tia_portal_cloud_v16
tia_portal_cloud_v17
tia_portal_cloud_v18
totally_integrated_automation_portal
totally_integrated_automation_portal__tia_portal__v15.1
totally_integrated_automation_portal__tia_portal__v16
totally_integrated_automation_portal__tia_portal__v17
totally_integrated_automation_portal__tia_portal__v18
totally_integrated_automation_portal__tia_portal__v19
wincc
wincc_tia_portal
simatic_s7-1500
simatic_s7
cpu_1518f-4_pn\/ dp_mfp_firmware
cpu_1518f-4_pn__dp_mfp_firmware

ruggedcom_ape1808_firmware
siemens_simatic_s7-1500_tm_mfp
siemens_simatic_s7_-1500_tm_mfp
siemens_telecontrol_server_basic
simatic_mv500_firmware
simatic_pcs_7
simatic_s7-1500_cpu_1518f-4_pn\/ dp_mfp_firmware
simatic_s7-1500_cpu_1518f-4_pn__dp_mfp_firmware
simatic_s7-1500_tm_mfp_firmware
simatic_step_7
simatic_wincc_oa

Disclaimer