Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0362

Kwetsbaarheden verholpen in Siemens producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 10-09-2024

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, SICAM, SIMATIC, SINEMA, SINUMERIK en Tecnomatix.

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
- 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-039007.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-097435.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-097786.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-103653.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-342438.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-359713.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-417159.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-423808.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-427715.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-446545.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-629254.pdf

- https://cert-portal.siemens.com/productcert/pdf/ssa-673996.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-765405.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-773256.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-869574.pdf

Kwetsbaarheden

CVE	CVSS Score
CVE-2006-5051	
CVE-2023-28827	5.9 MEDIUM
CVE-2023-30755	4.4 MEDIUM
CVE-2023-30756	5.9 MEDIUM
CVE-2023-46850	9.8 CRITICAL
CVE-2023-49069	5.3 MEDIUM
CVE-2024-2004	5.3 MEDIUM
CVE-2024-2379	
CVE-2024-2398	8.6 HIGH
CVE-2024-2466	7.1 HIGH
CVE-2024-6387	
CVE-2024-32006	4.3 MEDIUM
CVE-2024-33698	9.8 CRITICAL
CVE-2024-34057	8.2 HIGH
CVE-2024-35783	9.1 CRITICAL
CVE-2024-37990	6.5 MEDIUM
CVE-2024-37992	4.9 MEDIUM
CVE-2024-37993	5.3 MEDIUM

CVE-2024-37994	
CVE-2024-37995	2.7 LOW
CVE-2024-38355	7.3 HIGH
CVE-2024-41170	7.8 HIGH
CVE-2024-41171	8.8 HIGH
CVE-2024-42344	4.4 MEDIUM
CVE-2024-42345	
CVE-2024-43781	5.5 MEDIUM
CVE-2024-44087	8.6 HIGH
CVE-2024-45032	10.0 CRITICAL

CWE's

CWE	Beschrijving
CWE-115	Misinterpretation of Input
CWE-912	Hidden Functionality
CWE-364	Signal Handler Race Condition
CWE-772	Missing Release of Resource after Effective Lifetime
CWE-732	Incorrect Permission Assignment for Critical Resource
CWE-297	Improper Validation of Certificate with Host Mismatch
CWE-754	Improper Check for Unusual or Exceptional Conditions
CWE-703	Improper Check or Handling of Exceptional Conditions
CWE-319	Cleartext Transmission of Sensitive Information
CWE-613	Insufficient Session Expiration
CWE-190	Integer Overflow or Wraparound

CWE-532	Insertion of Sensitive Information into Log File
CWE-204	Observable Response Discrepancy
CWE-639	Authorization Bypass Through User-Controlled Key
CWE-250	Execution with Unnecessary Privileges
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-404	Improper Resource Shutdown or Release
CWE-284	Improper Access Control
CWE-416	Use After Free
CWE-401	Missing Release of Memory after Effective Lifetime
CWE-476	NULL Pointer Dereference
CWE-295	Improper Certificate Validation
CWE-384	Session Fixation
CWE-122	Heap-based Buffer Overflow
CWE-121	Stack-based Buffer Overflow
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-20	Improper Input Validation

Getroffen producten

siemens
ai_model_deployer
automation_license_manager_v5
automation_license_manager_v6.0
automation_license_manager_v6.2
data_flow_monitoring_industrial_edge_device_user_interface__dfm_ied_ui_
eti5_ethernet_int._1x100tx_iec61850

industrial_edge_management_os__iem-os_
industrial_edge_management_pro
industrial_edge_management_virtual
livetwin_industrial_edge_app__6av2170-0bl00-0aa0_
mendix_runtime_v10.12
mendix_runtime_v10.6
mendix_runtime_v10
mendix_runtime_v8
mendix_runtime_v9
sicam_scc
sicam_scc__10.0
simatic_batch_v9.1
simatic_cp_1242-7_v2__incl._siplus_variants_
simatic_cp_1243-1__incl._siplus_variants_
simatic_cp_1243-1_dnp3__incl._siplus_variants_
simatic_cp_1243-1_iec__incl._siplus_variants_
simatic_cp_1243-7_lte
simatic_cp_1243-8_irc
simatic_cp_1243-8_irc__6gk7243-8rx30-0xe0_
simatic_hmi_comfort_panels__incl._siplus_variants_
simatic_information_server_2020
simatic_information_server_2022
simatic_information_server_2024
simatic_ipc_diagbase
simatic_ipc_diagmonitor

simatic_pcs_7_v9.1
simatic_pcs_neo_v4.0
simatic_pcs_neo_v4.1
simatic_pcs_neo_v5.0
simatic_process_historian_2020
simatic_process_historian_2022
simatic_reader_rf610r_cmiit
simatic_reader_rf610r_cmiit__6gt2811-6bc10-2aa0_
simatic_reader_rf610r_etsi
simatic_reader_rf610r_etsi__6gt2811-6bc10-0aa0_
simatic_reader_rf610r_fcc
simatic_reader_rf610r_fcc__6gt2811-6bc10-1aa0_
simatic_reader_rf615r_cmiit
simatic_reader_rf615r_cmiit__6gt2811-6cc10-2aa0_
simatic_reader_rf615r_etsi
simatic_reader_rf615r_etsi__6gt2811-6cc10-0aa0_
simatic_reader_rf615r_fcc
simatic_reader_rf615r_fcc__6gt2811-6cc10-1aa0_
simatic_reader_rf650r_arib
simatic_reader_rf650r_arib__6gt2811-6ab20-4aa0_
simatic_reader_rf650r_cmiit
simatic_reader_rf650r_cmiit__6gt2811-6ab20-2aa0_
simatic_reader_rf650r_etsi
simatic_reader_rf650r_etsi__6gt2811-6ab20-0aa0_
simatic_reader_rf650r_fcc
simatic_reader_rf650r_fcc__6gt2811-6ab20-1aa0_

simatic_reader_rf680r_arib
simatic_reader_rf680r_arib__6gt2811-6aa10-4aa0_
simatic_reader_rf680r_cmiit
simatic_reader_rf680r_cmiit__6gt2811-6aa10-2aa0_
simatic_reader_rf680r_etsi
simatic_reader_rf680r_etsi__6gt2811-6aa10-0aa0_
simatic_reader_rf680r_fcc
simatic_reader_rf680r_fcc__6gt2811-6aa10-1aa0_
simatic_reader_rf685r_arib
simatic_reader_rf685r_arib__6gt2811-6ca10-4aa0_
simatic_reader_rf685r_cmiit
simatic_reader_rf685r_cmiit__6gt2811-6ca10-2aa0_
simatic_reader_rf685r_etsi
simatic_reader_rf685r_etsi__6gt2811-6ca10-0aa0_
simatic_reader_rf685r_fcc
simatic_reader_rf685r_fcc__6gt2811-6ca10-1aa0_
simatic_rf1140r
simatic_rf1140r__6gt2831-6cb00_
simatic_rf1170r
simatic_rf1170r__6gt2831-6bb00_
simatic_rf166c
simatic_rf166c__6gt2002-0ee20_
simatic_rf185c
simatic_rf185c__6gt2002-0je10_
simatic_rf186c
simatic_rf186c__6gt2002-0je20_

simatic_rf186ci
simatic_rf186ci__6gt2002-0je50_
simatic_rf188c
simatic_rf188c__6gt2002-0je40_
simatic_rf188ci
simatic_rf188ci__6gt2002-0je60_
simatic_rf360r
simatic_rf360r__6gt2801-5ba30_
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_wincc
simatic_wincc_runtime_advanced
simatic_wincc_runtime_professional_v17
simatic_wincc_runtime_professional_v18
simatic_wincc_runtime_professional_v19
simatic_wincc_runtime_professional_v20
simatic_wincc_v7.4
simatic_wincc_v7.5
simatic_wincc_v8.0
sinec_nms
sinema_remote_connect_client
sinema_remote_connect_server
sinumerik_828d_v4
sinumerik_828d_v5

sinumerik_840d_sl_v4
sinumerik_one
siplus_s7-1500_cpu_1518-4_pn_dp_mfp__6ag1518-4ax00-4ac0_
siplus_tim_1531_irc
siplus_tim_1531_irc__6ag1543-1mx00-7xe0_
sitipe_at
tecnomatix_plant_simulation_v2302
tecnomatix_plant_simulation_v2404
tia_administrator
tia_portal
tia_portal__v17_update_8
tia_portal_umc__v2.13.1
tim_1531_irc
tim_1531_irc__6gk7543-1mx00-0xe0_
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
sicam

Disclaimer