Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0246

Kwetsbaarheden verholpen in Siemens producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 11-06-2024

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, zoals SCALANCE, SICAM, Tecnomatix, SITOP en PowerSys.

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 beveiligingsmaatregel
- (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-024584.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-196737.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-238730.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-319319.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-337522.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-341067.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-481506.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-540640.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-620338.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-625862.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-690517.pdf
- https://cert-portal.siemens.com/productcert/pdf/ssa-879734.pdf

› https://cert-portal.siemens.com/productcert/pdf/ssa-900277.pdf

Kwetsbaarheden

CVE	CVSS Score
› CVE-2023-28319	
› CVE-2023-28484	
› CVE-2023-29331	
› CVE-2023-29469	
› CVE-2023-32032	
› CVE-2023-33126	
› CVE-2023-33127	
› CVE-2023-33128	
› CVE-2023-33135	
› CVE-2023-33170	
› CVE-2023-35390	
› CVE-2023-35391	
› CVE-2023-35788	
› CVE-2023-35823	
› CVE-2023-35824	
› CVE-2023-35828	
› CVE-2023-35829	
› CVE-2023-36038	
› CVE-2023-36049	

- CVE-2023-36435
- CVE-2023-36558
- CVE-2023-36792
- CVE-2023-36793
- CVE-2023-36794
- CVE-2023-36796
- CVE-2023-36799
- CVE-2023-38171
- CVE-2023-38178
- CVE-2023-38180
- CVE-2023-38380
- CVE-2023-38533
- CVE-2023-39615
- CVE-2023-41910
- CVE-2023-44317
- CVE-2023-44318
- CVE-2023-44319
- CVE-2023-44373
- CVE-2023-44374
- CVE-2023-44487
- CVE-2023-49691
- CVE-2023-50763
- CVE-2023-52474

- CVE-2024-0775
- CVE-2024-31484
- CVE-2024-33500
- CVE-2024-35206
- CVE-2024-35207
- CVE-2024-35208
- CVE-2024-35209
- CVE-2024-35210
- CVE-2024-35211
- CVE-2024-35212
- CVE-2024-35292
- CVE-2024-35303 **7.8 HIGH**
- CVE-2024-36266
- CVE-2021-47178
- CVE-2022-1015
- CVE-2022-2097
- CVE-2022-3435
- CVE-2022-3545
- CVE-2022-3623
- CVE-2022-3643
- CVE-2022-4304
- CVE-2022-4450
- CVE-2022-36323

- CVE-2022-39189
- CVE-2022-40225
- CVE-2022-40303
- CVE-2022-40304
- CVE-2022-41742
- CVE-2022-42328
- CVE-2022-42329
- CVE-2022-44792
- CVE-2022-44793
- CVE-2022-45886
- CVE-2022-45887
- CVE-2022-45919
- CVE-2022-46144
- CVE-2023-0160
- CVE-2023-0215
- CVE-2023-0286
- CVE-2023-0464
- CVE-2023-0465
- CVE-2023-0466
- CVE-2023-1017
- CVE-2023-2124
- CVE-2023-2269
- CVE-2023-3446

- CVE-2023-3817
- CVE-2023-5678
- CVE-2023-21255
- CVE-2023-21808
- CVE-2023-24895
- CVE-2023-24897
- CVE-2023-24936
- CVE-2023-26552
- CVE-2023-26553
- CVE-2023-26554
- CVE-2023-27321
- CVE-2023-28260

CWE's

CWE	Beschrijving
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
CWE-121	Stack-based Buffer Overflow
CWE-122	Heap-based Buffer Overflow
CWE-1220	Insufficient Granularity of Access Control
CWE-123	Write-what-where Condition
CWE-125	Out-of-bounds Read
CWE-1333	Inefficient Regular Expression Complexity
CWE-170	Improper Null Termination
CWE-190	Integer Overflow or Wraparound

CWE-191	Integer Underflow (Wrap or Wraparound)
CWE-20	Improper Input Validation
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-269	Improper Privilege Management
CWE-287	Improper Authentication
CWE-295	Improper Certificate Validation
CWE-311	Missing Encryption of Sensitive Data
CWE-319	Cleartext Transmission of Sensitive Information
CWE-321	Use of Hard-coded Cryptographic Key
CWE-325	Missing Cryptographic Step
CWE-326	Inadequate Encryption Strength
CWE-328	Use of Weak Hash
CWE-330	Use of Insufficiently Random Values
CWE-349	Acceptance of Extraneous Untrusted Data With Trusted Data
CWE-352	Cross-Site Request Forgery (CSRF)
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-379	Creation of Temporary File in Directory with Insecure Permissions
CWE-400	Uncontrolled Resource Consumption
CWE-401	Missing Release of Memory after Effective Lifetime
CWE-404	Improper Resource Shutdown or Release
CWE-415	Double Free
CWE-416	Use After Free
CWE-476	NULL Pointer Dereference
CWE-522	Insufficiently Protected Credentials
CWE-567	Unsynchronized Access to Shared Data in a Multithreaded Context

CWE-613	Insufficient Session Expiration
CWE-614	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute
CWE-664	Improper Control of a Resource Through its Lifetime
CWE-667	Improper Locking
CWE-704	Incorrect Type Conversion or Cast
CWE-74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')
CWE-749	Exposed Dangerous Method or Function
CWE-754	Improper Check for Unusual or Exceptional Conditions
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-787	Out-of-bounds Write
CWE-833	Deadlock
CWE-834	Excessive Iteration
CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')
CWE-94	Improper Control of Generation of Code ('Code Injection')

Getroffen producten

siemens
mendix
simatic
sinec-nms
tecnomatix_plant_simulation
tia_administrator

scalance_w700
scalance_xm-400
scalance_xr-500
sicam_ak_3
sicam_bc
sicam_tm
siplus_tim_1531_irc
sitop_ups1600

Disclaimer