ROYAUME DU MAROC

ADMINISTRATION
DE LA DEFENSE NATIONALE

Direction Générale de la Sécurité des Systèmes d'Information

Centre de Veille de Détection et de Réaction aux Attaques Informatiques

المملكة المغربية

إدارة الدفاع الوطني

المديرية العامة لأمن نظم المعلومات

مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

BULLETIN DE SECURITE

Titre	Vulnérabilités affectant des produits de Siemens
Numéro de Référence	63261604/26
Date de Publication	16 Avril 2026
Risque	Important
Impact	Important

Systèmes affectés

- Siemens Software Center – versions antérieures à V3.5.8.2
- Simcenter 3D – versions antérieures à V2506.6000
- Simcenter Femap – versions antérieures à V2506.0002
- Simcenter STAR-CCM+ – versions antérieures à V2602
- Solid Edge SE2025 – versions antérieures à V225.0 Update 13
- Solid Edge SE2026 – versions antérieures à V226.0 Update 04
- Tecnomatix Plant Simulation – versions antérieures à V2504.0008
- SINEC NMS – versions antérieures à V4.0 SP3 with UMC
- RUGGEDCOM CROSSBOW Secure Access Manager Primary (SAM-P) – versions antérieures à V5.8
- SIPROTEC 5 - CP300 Devices – multiple versions and models
- SIPROTEC 5 Communication Modules – multiple versions and models
- SIPROTEC 5 Compact 7SX800 (CP050) – de la version V8.70 jusqu'à la version V9.30
- SIMATIC CN 4100 – hardware versions antérieures à FS 05
- SIMATIC Field PG – all versions
- SIMATIC IPC family – all versions
- SIMATIC IPC MD-57A – versions antérieures à V30.01.10
- SIMATIC ITP1000 – all versions
- Industrial Edge Management Pro V1 – de la version V1.7.6 jusqu'à la version V1.15.17
- Industrial Edge Management Pro V2 – de la version V2.0.0 jusqu'à la version V2.1.1
- Industrial Edge Management Virtual – de la version V2.2.0 jusqu'à la version V2.8.0
- SINEC NMS – versions antérieures à V4.0 SP3

- RUGGEDCOM CROSSBOW Station Access Controller (SAC) – versions antérieures à V5.8
- SCALANCE W-700 IEEE 802.11n family – versions antérieures à V6.6.0

Identificateurs externes

CVE-2020-24588 CVE-2020-26139 CVE-2020-26140 CVE-2020-26141 CVE-2020-26143 CVE-2020-26144 CVE-2020-26146 CVE-2020-26147 CVE-2021-3712 CVE-2022-0778 CVE-2022-31765 CVE-2022-36323 CVE-2022-36324 CVE-2022-36325 CVE-2023-44373 CVE-2025-2884

Bilan de la vulnérabilité

Siemens annonce la correction de plusieurs vulnérabilités affectant ses produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant d'exécuter du code à distance d'accéder à des données confidentielles, de contourner les mesures de sécurité, d'élever ses privilèges ou de causer un déni de service.

Solution

Veuillez se référer aux bulletins de sécurité de Siemens pour mettre à jour vos produits.

Risques

- Exécution de code à distance
- Accès à des données confidentielles
- Contournement de mesures de sécurité
- Elévation de privilèges
- Déni de service.

Références

Bulletins de sécurité de Siemens:

- https://cert-portal.siemens.com/productcert/html/ssa-019200.html
- https://cert-portal.siemens.com/productcert/html/ssa-186293.html
- https://cert-portal.siemens.com/productcert/html/ssa-216014.html
- https://cert-portal.siemens.com/productcert/html/ssa-225816.html

- https://cert-portal.siemens.com/productcert/html/ssa-244969.html
- https://cert-portal.siemens.com/productcert/html/ssa-311973.html
- https://cert-portal.siemens.com/productcert/html/ssa-408105.html
- https://cert-portal.siemens.com/productcert/html/ssa-552702.html
- https://cert-portal.siemens.com/productcert/html/ssa-599968.html
- https://cert-portal.siemens.com/productcert/html/ssa-605717.html
- https://cert-portal.siemens.com/productcert/html/ssa-609469.html
- https://cert-portal.siemens.com/productcert/html/ssa-628843.html
- https://cert-portal.siemens.com/productcert/html/ssa-710008.html
- https://cert-portal.siemens.com/productcert/html/ssa-712929.html
- https://cert-portal.siemens.com/productcert/html/ssa-726617.html
- https://cert-portal.siemens.com/productcert/html/ssa-726834.html
- https://cert-portal.siemens.com/productcert/html/ssa-741509.html
- https://cert-portal.siemens.com/productcert/html/ssa-801704.html
- https://cert-portal.siemens.com/productcert/html/ssa-827968.html
- https://cert-portal.siemens.com/productcert/html/ssa-913875.html
- https://cert-portal.siemens.com/productcert/html/ssa-981622.html

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques
Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية
هاتف: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma