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	59231112/25
Date de Publication	11 décembre 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- Building X - Security Manager Edge Controller (ACC-AP) – toutes les versions
- COMOS V10.6 – toutes les versions
- COMOS – plusieurs versions
- Energy Services G5DFR – versions antérieures à G5DFR to V1.2.3.13
- Gridscale X Prepay – versions antérieures à V4.2.1
- Interniche IP-Stack - plusieurs versions et plateformes
- JT Bi-Directional Translator for STEP – toutes les versions
- NX V2412 – versions antérieures à V2412.8700
- NX V2412 – versions antérieures à V2506.6000
- NX V2506 – versions antérieures à V2506.6000
- RUGGEDCOM ROS V5.X family – versions antérieures à V5.10.1
- RUGGEDCOM ROX II family – versions antérieures à V2.17.0
- SICAM T – versions antérieures à V3.0
- SIMATIC CN 4100 – versions antérieures à V4.0.1
- SINEC Security Monitor – versions antérieures à V4.10.0
- SINEMA Remote Connect Server – versions antérieures à V3.2 SP4
- Simcenter 3D – versions antérieures à V2506.6000
- Simcenter Femap – versions antérieures à V2506.0002
- Simcenter Studio – toutes les versions
- Simcenter System Architect – toutes les versions
- Solid Edge SE2025 – versions antérieures à V225.0 Update 10
- Solid Edge SE2026 – versions antérieures à V226.0 Update 1
- Tecnomatix Plant Simulation – versions antérieures à V2504.0007

Identificateurs externes

CVE-2022-29872 CVE-2022-29873 CVE-2022-29874 CVE-2022-29876 CVE-2022-29878
CVE-2022-29879 CVE-2022-29880 CVE-2022-29881 CVE-2022-29882 CVE-2022-29883
CVE-2022-40226 CVE-2022-41665 CVE-2022-43439 CVE-2023-30901 CVE-2023-31238
CVE-2025-40820 CVE-2025-40937 CVE-2025-40938 CVE-2025-40939 CVE-2025-40940
CVE-2025-40941

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 de contourner les mesures de sécurité, d'exécuter du code arbitraire à distance, d'injecter du code à distance, d'accéder à des données confidentielles ou de causer un déni de service à distance.

Solution

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

Risques

- Contournement de mesures de sécurité
- Déni de service à distance
- Exécution de code arbitraire à distance
- Injection de code à distance
- Accès à des données confidentielles

Références

Bulletins de sécurité de Siemens:

- https://www.siemens.com/global/en/products/services/cert.html#SecurityPublications