ROYAUME DU MAROC

ADMINISTRATION
DE LA DEFENSE NATIONALE

Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية

إدارة الدفاع الوطني

المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Vulnérabilités dans les produits Siemens
Numéro de Référence	39741301/23
Date de Publication	13 janvier 2023
Risque	Important
Impact	Important

Systèmes affectés

- Automation License Manager V5
- Automation License Manager versions V6 antérieures à V6 SP9 Upd4
- De nombreux produits SIMATIC, SIMOTION, SINAMICS, SINUMERIK et SIPLUS (Se référer au bulletin de sécurité de l'éditeur pour les versions affectées)
- Development/Evaluation Kits for PROFINET IO: DK Standard Ethernet Controller versions antérieures à V4.1.1 Patch 05
- Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200 versions antérieures à V4.5.0 Patch 01
- Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200P versions antérieures à V4.5.0
- JT Open versions antérieures à V11.1.1.0
- JT Open versions antérieures à V13.1.1.0
- Mendix SAML (Mendix 8 compatible) versions V2.3.x antérieures à V2.3.4
- Mendix SAML (Mendix 9 compatible, New Track) versions V3.3.x antérieures à V3.3.9
- Mendix SAML (Mendix 9 compatible, Upgrade Track) versions V3.3.x antérieures à V3.3.8
- SCALANCE X-200IRT switch family (incl. SIPLUS NET variants) versions antérieures à V5.4.2
- SINEC INS versions antérieures à V1.0 SP2 Update 1
- Solid Edge versions antérieures à V2023 MP1

Identificateurs externes

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – 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 ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

- CVE-2022-2068 , CVE-2022-1292 , CVE-2022-2097 , CVE-2022-2274 , CVE-2022-32212 , CVE-2022-32213 , CVE-2022-32215 , CVE-2022-32222 , CVE-2022-35255 , CVE-2022-35256 , CVE-2022-45092 , CVE-2022-45093 , CVE-2022-45094 , CVE-2019-10923 , CVE-2019-13940 , CVE-2022-43513 , CVE-2022-43514 , CVE-2022-38773 , CVE-2022-46823 , CVE-2018-4843 , CVE-2021-44002 , CVE-2021-44014 , CVE-2022-47935 , CVE-2022-47967

Bilan de la vulnérabilité

Plusieurs vulnérabilités ont été corrigées dans les systèmes industriels de Siemens susmentionnés. Un attaquant pourrait exploiter ces failles afin d'exécuter du code arbitraire à distance, réussir une élévation de privilèges, causer un déni de service, contourner la politique de sécurité ou porter atteinte à la confidentialité de données.

Solution

Veuillez se référer au bulletin de sécurité Siemens du 10 janvier 2023 pour plus d'information.

Risque

- Exécution de code arbitraire à distance
- Elévation de privilèges
- Déni de service
- Contournement de la politique de sécurité
- Atteinte à la confidentialité de données

Annexe

Bulletin de sécurité Siemens du 10 janvier 2023 :

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