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 industriels de Siemens
Numéro de Référence	40942203/23
Date de Publication	22 Mars 2023
Risque	Important
Impact	Important

Systèmes affectés

- Mendix SAML (Mendix 7 compatible) versions antérieures à V1.17.3
- Mendix SAML (Mendix 8 compatible) versions antérieures à V2.3.0
- Mendix SAML (Mendix 9 compatible, New Track) versions 3.1.9 à 3.2.x antérieures à V3.3.0
- Mendix SAML (Mendix 9 compatible, Upgrade Track) versions 3.1.9 à 3.2.x antérieures à V3.3.0
- RUGGEDCOM CROSSBOW versions antérieures à V5.3
- RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2) et NAM (6GK6108-4AM00-2DA2) versions antérieures à V7.2
- SINEC NMS
- SINEMA Server V14
- SCALANCE et SIPROTEC

Identificateurs externes

- CVE-2022-4304 , CVE-2022-4450 , CVE-2023-0215 , CVE-2023-0286 , CVE-2022-24281 , CVE-2022-24282 , CVE-2022-25311 , CVE-2023-27309 , CVE-2023-27310 , CVE-2023-27462 , CVE-2023-27463 , CVE-2018-25032 , CVE-2019-1125 , CVE-2019-1071 , CVE-2019-1073 , CVE-2021-4034 , CVE-2021-4149 , CVE-2021-26401 , CVE-2017-5715 , CVE-2021-42373 , CVE-2021-42374 , CVE-2021-42375 , CVE-2021-42376 , CVE-2021-42377 , CVE-2021-42378 , CVE-2021-42379 , CVE-2021-42380 , CVE-2021-42381 , CVE-2021-42382 , CVE-2021-42383 , CVE-2021-42384 , CVE-2021-42385 , CVE-2021-42386 , CVE-2022-0001 , CVE-2022-0002 , CVE-2022-0494 , CVE-2022-0547 , CVE-2022-1011 , CVE-2022-1016 , CVE-2022-1198 , CVE-2022-1199 , CVE-2022-1292 , CVE-2022-1304 , CVE-2022-1343 , CVE-2022-1353 , CVE-2022-1473 , CVE-2022-1516 , CVE-2022-1652 , CVE-2022-1729 , CVE-2022-

1734 , CVE-2022-1974 , CVE-2022-1975 , CVE-2022-2380 , CVE-2022-2588 , CVE-2022-2639 , CVE-2022-20158 , CVE-2022-23036 , CVE-2022-23037 , CVE-2022-23038 , CVE-2022-23039 , CVE-2022-23040 , CVE-2022-23041 , CVE-2022-23042 , CVE-2022-23308 , CVE-2022-26490 , CVE-2022-28356 , CVE-2022-28390 , CVE-2022-30065 , CVE-2022-30594 , CVE-2022-32205 , CVE-2022-32206 , CVE-2022-32207 , CVE-2022-32208 , CVE-2022-32296 , CVE-2022-32981 , CVE-2022-33981 , CVE-2022-35252 , CVE-2022-36879 , CVE-2022-36946 , CVE-2018-12886 , CVE-2022-23395 , CVE-2022-38767 , CVE-2023-25957

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 de Mars 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 de Mars 2023 :

- https://cert-portal.siemens.com/productcert/html/ssa-203374.html
- https://cert-portal.siemens.com/productcert/html/ssa-250085.html
- https://cert-portal.siemens.com/productcert/html/ssa-260625.html
- https://cert-portal.siemens.com/productcert/html/ssa-320629.html
- https://cert-portal.siemens.com/productcert/html/ssa-419740.html
- https://cert-portal.siemens.com/productcert/html/ssa-565386.html
- https://cert-portal.siemens.com/productcert/html/ssa-726834.html
- https://cert-portal.siemens.com/productcert/html/ssa-851884.html

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: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma