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	47411405/24
Date de Publication	14 Mai 2024
Risque	Important
Impact	Important

Systèmes affectés

- Totally Integrated Automation Portal (TIA Portal) V19 versions antérieures à V19 Update 2
- Totally Integrated Automation Portal (TIA Portal) V18 toutes versions
- Totally Integrated Automation Portal (TIA Portal) V17 toutes versions
- Totally Integrated Automation Portal (TIA Portal) V16 toutes versions. L'éditeur indique que le produit ne bénéficiera pas de correctif de sécurité pour la vulnérabilité CVE-2023-46280
- Totally Integrated Automation Portal (TIA Portal) V15.1 toutes versions. L'éditeur indique que le produit ne bénéficiera pas de correctif de sécurité pour la vulnérabilité CVE-2023-46280
- TIA Portal Cloud Connector versions antérieures à V2.0
- Sicam SICORE Base system versions antérieures à V1.3.0
- Sicam OPUPI0 AMQP/MQTT versions antérieures à V5.30
- Sicam CPCI85 Central Processing/Communication versions antérieures à V5.30
- Sicam CPC80 Central Processing/Communication versions antérieures à V16.41
- SIMATIC WinCC V8.0 toutes versions
- SIMATIC WinCC V7.5 toutes versions
- SIMATIC WinCC V7.4 toutes versions. L'éditeur indique que le produit ne bénéficiera pas de correctif de sécurité pour la vulnérabilité CVE-2023-46280
- SIMATIC WinCC Unified PC Runtime toutes versions
- SIMATIC WinCC Runtime Professional V19 toutes versions
- SIMATIC WinCC Runtime Professional V18 toutes versions

- SIMATIC WinCC Runtime Professional V17 toutes versions
- SIMATIC WinCC Runtime Professional V16 toutes versions
- SIMATIC WinCC Runtime Advanced toutes versions
- SIMATIC WinCC OA V3.19 versions antérieures à V3.19 P010
- SIMATIC WinCC OA V3.18 versions antérieures à V3.18 P025
- SIMATIC WinCC OA V3.17 toutes versions. L'éditeur indique que le produit ne bénéficiera pas de correctif de sécurité pour la vulnérabilité CVE-2023-46280
- SIMATIC STEP 7 V5 toutes versions
- SIMATIC Route Control V9.1 toutes versions
- SIMATIC PDM V9.2 toutes versions
- SIMATIC PCS 7 V9.1 toutes versions
- SIMATIC NET PC Software toutes versions
- SIMATIC CN 4100 versions antérieures à V3.0
- SIMATIC BATCH V9.1 toutes versions
- SIMATIC Automation Tool toutes versions
- S7-PCT toutes versions

Identificateurs externes

- CVE-2023-46280 CVE-2024-31484 CVE-2024-31485 CVE-2024-31486 CVE-2024-32740 CVE-2024-32741 CVE-2024-32742

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 13 Mai 2024 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 13 Mai 2024:

- https://cert-portal.siemens.com/productcert/html/ssa-273900.html
- https://cert-portal.siemens.com/productcert/html/ssa-871704.html
- https://cert-portal.siemens.com/productcert/html/ssa-962515.html