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 Siemens
Numéro de Référence	37311407/22
Date de Publication	14 Juillet 2022
Risque	Important
Impact	Important

Systèmes affectés

- Opcenter Quality versions 13.1 antérieures à 13.1.20220624
- Opcenter Quality versions 13.2 antérieures à 13.2.20220624
- Disques SINAMICS PERFECT HARMONY GH180 Drives fabriqués depuis 2015 avant 2021
- EN100 Ethernet module DNP3 IP variant toutes versions
- EN100 Ethernet module IEC 104 variant toutes versions
- EN100 Ethernet module IEC 61850 variant versions antérieures à 4.40
- EN100 Ethernet module Modbus TCP variant toutes versions
- EN100 Ethernet module PROFINET IO variant toutes versions
- RUGGEDCOM ROS toutes versions : Se référer à l'avis éditeur pour la liste exacte des produits RUGGEDCOM concernés et des correctifs disponibles
- JT2Go versions antérieures à 13.3.0.5
- Teamcenter Visualization versions 13.3.x antérieures à 13.3.0.5
- Teamcenter Visualization toutes versions 14.0.x
- Mendix Excel Importer Module (Mendix 8 compatible) versions antérieures à 9.2.2
- Mendix Excel Importer Module (Mendix 9 compatible) versions antérieures à 10.1.2
- RUGGEDCOM ROX MX5000 à RX5000 versions antérieures à 2.15.1
- SIMATIC eaSie Core Package (6DL5424-0AX00-0AV8) versions antérieures à 22.00
- SIMATIC CP 1242-7 V2 (6GK7242-7KX31-0XE0) à SIMATIC CP 1243-8 IRC (6GK7243-8RX30-0XE0) toutes versions
- SIMATIC CP 1542SP-1 IRC (6GK7542-6VX00-0XE0) versions antérieures à 2.0
- SIMATIC CP 1543-1 (6GK7543-1AX00-0XE0) versions antérieures à 3.0.22
- SIMATIC CP 1543SP-1 (6GK7543-6WX00-0XE0) versions antérieures à 2.0
- SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (6AG2542-6VX00-4XE0) versions antérieures à 2.0

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

- SIPLUS ET 200SP CP 1543SP-1 ISEC (6AG1543-6WX00-7XE0) versions antérieures à 2.0
- SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (6AG2543-6WX00-4XE0) versions antérieures à 2.0
- SIPLUS NET CP 1242-7 V2 (6AG1242-7KX31-7XE0) toutes versions
- SIPLUS NET CP 1543-1 (6AG1543-1AX00-2XE0) versions antérieures à 3.0.22
- SIPLUS S7-1200 CP 1243-1 (6AG1243-1BX30-2AX0) toutes versions
- SIPLUS S7-1200 CP 1243-1 RAIL (6AG2243-1BX30-1XE0) toutes versions : Se référer à l'avis éditeur pour la liste exacte des produits SIMATIC concernés et des correctifs disponibles
- Mendix Applications using Mendix 9 versions supérieures ou égales à 9.11 et antérieures à 9.15
- Mendix Applications using Mendix 9 versions 9.12 antérieure à 9.12.3
- CP-8000 MASTER MODULE WITH I/O -25/+70°C (6MF2101-0AB10-0AA0) versions antérieures à CPC80 V16.30
- CP-8000 MASTER MODULE WITH I/O -40/+70°C (6MF2101-1AB10-0AA0) versions antérieures à CPC80 V16.30
- CP-8021 MASTER MODULE (6MF2802-1AA00) versions antérieures à CPC80 V16.30
- CP-8022 MASTER MODULE WITH GPRS (6MF2802-2AA00) versions antérieures à CPC80 V16.30
- Simcenter Femap versions antérieures à 2022.2
- PADS Standard/Plus Viewer toutes versions
- Mendix Applications using Mendix versions 7 antérieures à 7.23.31
- Mendix Applications using Mendix versions 8 antérieures à 8.18.18
- Mendix Applications using Mendix versions 9 antérieures à 9.14.0
- Mendix Applications using Mendix versions 9 (9.6) antérieures à 9.6.12
- Mendix Applications using Mendix versions 9 (9.12) antérieures à 9.12.2
- Teamcenter Visualization V12.4 toutes versions
- Teamcenter Visualization V13.2 toutes versions
- Teamcenter Visualization V14.0 toutes versions
- SIMATIC MV540 H (6GF3540-0GE10) versions antérieures à 3.3
- SIMATIC MV540 S (6GF3540-0CD10) versions antérieures à 3.3
- SIMATIC MV550 H (6GF3550-0GE10) versions antérieures à 3.3
- SIMATIC MV550 S (6GF3550-0CD10) versions antérieures à 3.3
- SIMATIC MV560 U (6GF3560-0LE10) versions antérieures à 3.3
- SIMATIC MV560 X (6GF3560-0HE10) versions antérieures à 3.3
- SCALANCE X200-4P IRT (6GK5200-4AH00-2BA3) à SCALANCE X200-4P IRT (6GK5200-4AH00-2BA3) toutes versions : Se référer à l'avis éditeur pour la liste exacte des produits SCALANCE concernés et des correctifs disponibles
- Parasolid V33.1 toutes versions
- Parasolid V34.0 versions antérieures à 34.0.250
- Parasolid V34.1 versions antérieures à 34.1.233
- Simcenter Femap toutes versions
- SICAM GridEdge Essential ARM (6MD7881-2AA30) toutes versions

- SICAM GridEdge Essential Intel (6MD7881-2AA40) versions antérieures à 2.7.3
- SICAM GridEdge Essential with GDS ARM (6MD7881-2AA10) toutes versions
- SICAM GridEdge Essential with GDS Intel (6MD7881-2AA20) versions antérieures à 2.7.3

Identificateurs externes

- CVE-2021-29998 CVE-2022-33736 CVE-2022-30938 CVE-2022-34663 CVE-2022-34467 CVE-2022-29560 CVE-2021-44221 CVE-2021-44222 CVE-2022-34819 CVE-2022-34820 CVE-2022-34821 CVE-2022-34466 CVE-2022-29884 CVE-2022-34748 CVE-2022-34272 CVE-2022-34273 CVE-2022-34274 CVE-2022-34275 CVE-2022-34276 CVE-2022-34277 CVE-2022-34278 CVE-2022-34279 CVE-2022-34280 CVE-2022-34281 CVE-2022-34282 CVE-2022-34283 CVE-2022-34284 CVE-2022-34285 CVE-2022-34286 CVE-2022-34287 CVE-2022-34288 CVE-2022-34289 CVE-2022-34290 CVE-2022-34291 CVE-2022-31257 CVE-2022-28807 CVE-2022-28808 CVE-2022-28809 CVE-2022-33137 CVE-2022-33138 CVE-2022-26647 CVE-2022-26648 CVE-2022-26649 CVE-2022-34465 CVE-2022-34464

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 12 Juillet 2022 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 12 Juillet 2022 :

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