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	36951706/22
Date de Publication	17 juin 2022
Risque	Important
Impact	Important

Systèmes affectés

- APOGEE PXC Compact (BACnet) versions antérieures à V3.5
- APOGEE PXC Compact (P2 Ethernet) toutes versions
- APOGEE PXC Modular (BACnet) versions antérieures à V3.5
- APOGEE PXC Modular (P2 Ethernet) toutes versions
- 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 V4.37
- EN100 Ethernet module Modbus TCP variant toutes versions
- EN100 Ethernet module PROFINET IO variant toutes versions
- Industrial Edge - OPC UA Connector toutes versions
- Industrial Edge - PROFINET IO Connector toutes versions
- Industrial Edge - SIMATIC S7 Connector App versions antérieures à V1.7.0
- Mendix SAML Module (Mendix 7 compatible) versions antérieures à 1.16.6
- Mendix SAML Module (Mendix 8 compatible) versions antérieures à 2.2.2
- Mendix SAML Module (Mendix 9 compatible) versions antérieures à 3.2.3
- RUGGEDCOM CROSSBOW Station Access Controller toutes versions
- RUGGEDCOM NMS toutes versions
- RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2) toutes versions
- RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2) toutes versions
- RUGGEDCOM ROS Series toutes versions
- RUGGEDCOM ROX Series toutes versions
- SCALANCE LPE9403 (6GK5998-3GS00-2AC2) versions antérieures à V2.0
- SCALANCE LPE9403 (6GK5998-3GS00-2AC2) versions antérieures à V2.0
- SCALANCE LPE9403 (6GK5998-3GS00-2AC2) versions antérieures à V2.0
- SCALANCE M804PB (6GK5804-0AP00-2AA2) toutes versions

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

- SCALANCE M812-1 ADSL-Router (Annex A) (6GK5812-1AA00-2AA2) toutes versions
- SCALANCE M812-1 ADSL-Router (Annex B) (6GK5812-1BA00-2AA2) toutes versions
- SCALANCE M816-1 ADSL-Router (Annex A) (6GK5816-1AA00-2AA2) toutes versions
- SCALANCE M816-1 ADSL-Router (Annex B) (6GK5816-1BA00-2AA2) toutes versions
- SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2) toutes versions
- SCALANCE M874-2 (6GK5874-2AA00-2AA2) toutes versions
- SCALANCE M874-3 (6GK5874-3AA00-2AA2) toutes versions
- SCALANCE M876-3 (EVDO) (6GK5876-3AA02-2BA2) toutes versions
- SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2) toutes versions
- SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2) toutes versions
- SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2) toutes versions
- SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1) toutes versions
- SCALANCE MUM853-1 (RoW) (6GK5853-2EA00-2AA1) toutes versions
- SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1) toutes versions
- SCALANCE MUM856-1 (NAM) (6GK5856-2EA00-3BA1) toutes versions
- SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1) toutes versions
- SCALANCE S615 (6GK5615-0AA00-2AA2) toutes versions
- SCALANCE SC622-2C (6GK5622-2GS00-2AC2) toutes versions versions antérieures à V2.3.1
- SCALANCE SC632-2C (6GK5632-2GS00-2AC2) toutes versions versions antérieures à V2.3.1
- SCALANCE SC636-2C (6GK5636-2GS00-2AC2) toutes versions versions antérieures à V2.3.1
- SCALANCE SC642-2C (6GK5642-2GS00-2AC2) toutes versions versions antérieures à V2.3.1
- SCALANCE SC646-2C (6GK5646-2GS00-2AC2) toutes versions versions antérieures à V2.3.1
- SCALANCE XM408-4C (6GK5408-4GP00-2AM2) versions antérieures à V6.5
- SCALANCE XM408-4C (L3 int.) (6GK5408-4GQ00-2AM2) versions antérieures à V6.5
- SCALANCE XM408-8C (6GK5408-8GS00-2AM2) versions antérieures à V6.5
- SCALANCE XM408-8C (L3 int.) (6GK5408-8GR00-2AM2) versions antérieures à V6.5
- SCALANCE XM416-4C (6GK5416-4GS00-2AM2) versions antérieures à V6.5
- SCALANCE XM416-4C (L3 int.) (6GK5416-4GR00-2AM2) versions antérieures à V6.5
- SCALANCE XR524-8C, 1x230V (6GK5524-8GS00-3AR2) versions antérieures à V6.5
- SCALANCE XR524-8C, 1x230V (L3 int.) (6GK5524-8GR00-3AR2) versions antérieures à V6.5
- SCALANCE XR524-8C, 24V (6GK5524-8GS00-2AR2) versions antérieures à V6.5

- SCALANCE XR524-8C, 24V (L3 int.) (6GK5524-8GR00-2AR2) versions antérieures à V6.5
- SCALANCE XR524-8C, 2x230V (6GK5524-8GS00-4AR2) versions antérieures à V6.5
- SCALANCE XR524-8C, 2x230V (L3 int.) (6GK5524-8GR00-4AR2) versions antérieures à V6.5
- SCALANCE XR526-8C, 1x230V (6GK5526-8GS00-3AR2) versions antérieures à V6.5
- SCALANCE XR526-8C, 1x230V (L3 int.) (6GK5526-8GR00-3AR2) versions antérieures à V6.5
- SCALANCE XR526-8C, 24V (6GK5526-8GS00-2AR2) versions antérieures à V6.5
- SCALANCE XR526-8C, 24V (L3 int.) (6GK5526-8GR00-2AR2) versions antérieures à V6.5
- SCALANCE XR526-8C, 2x230V (6GK5526-8GS00-4AR2) versions antérieures à V6.5
- SCALANCE XR526-8C, 2x230V (L3 int.) (6GK5526-8GR00-4AR2) versions antérieures à V6.5
- SCALANCE XR528-6M (2HR2) (6GK5528-0AA00-2HR2) versions antérieures à V6.5
- SCALANCE XR528-6M (2HR2, L3 int.) (6GK5528-0AR00-2HR2) versions antérieures à V6.5
- SCALANCE XR528-6M (6GK5528-0AA00-2AR2) versions antérieures à V6.5
- SCALANCE XR528-6M (L3 int.) (6GK5528-0AR00-2AR2) versions antérieures à V6.5
- SCALANCE XR552-12M (2HR2) (6GK5552-0AA00-2HR2) versions antérieures à V6.5
- SCALANCE XR552-12M (2HR2) (6GK5552-0AR00-2HR2) versions antérieures à V6.5
- SCALANCE XR552-12M (2HR2, L3 int.) (6GK5552-0AR00-2AR2) versions antérieures à V6.5
- SCALANCE XR552-12M (6GK5552-0AA00-2AR2) versions antérieures à V6.5
- SICAM GridEdge Essential ARM (6MD7881-2AA30) versions antérieures à V2.6.6
- SICAM GridEdge Essential Intel (6MD7881-2AA40) versions antérieures à V2.6.6
- SICAM GridEdge Essential with GDS ARM (6MD7881-2AA10) versions antérieures à V2.6.6
- SICAM GridEdge Essential with GDS Intel (6MD7881-2AA20) versions antérieures à V2.6.6
- SIMATIC Cloud Connect 7 CC712 (6GK1411-1AC00) toutes versions
- SIMATIC Cloud Connect 7 CC716 (6GK1411-5AC00) toutes versions
- SIMATIC CP 1242-7 V2 (6GK7242-7KX31-0XE0) toutes versions
- SIMATIC CP 1243-1 (6GK7243-1BX30-0XE0) toutes versions
- SIMATIC CP 1243-7 LTE EU (6GK7243-7KX30-0XE0) toutes versions
- SIMATIC CP 1243-7 LTE US (6GK7243-7SX30-0XE0) toutes versions
- SIMATIC CP 1243-8 IRC (6GK7243-8RX30-0XE0) toutes versions
- SIMATIC CP 1542SP-1 (6GK7542-6UX00-0XE0) toutes versions
- SIMATIC CP 1543-1 (6GK7543-1AX00-0XE0) toutes versions
- SIMATIC CP 1543-1 (incl. SIPLUS variants) versions antérieures à V3.0
- SIMATIC CP 1543SP-1 (6GK7543-6WX00-0XE0) toutes versions
- SIMATIC CP 1545-1 (6GK7545-1GX00-0XE0) toutes versions
- SIMATIC CP 1545-1 (6GK7545-1GX00-0XE0) versions antérieures à V1.1

- SIMATIC CP 1626 (6GK1162-6AA01) toutes versions
- SIMATIC CP 1628 (6GK1162-8AA00) toutes versions
- SIMATIC CP 343-1 Advanced (6GK7343-1GX31-0XE0) toutes versions
- SIMATIC CP 443-1 Advanced (6GK7443-1GX30-0XE0) toutes versions
- SIMATIC CP 443-1 OPC UA (6GK7443-1UX00-0XE0) toutes versions
- SIMATIC ET 200SP Open Controller (incl. SIPLUS variants) toutes versions
- SIMATIC Logon toutes versions
- SIMATIC MV540 H (6GF3540-0GE10) toutes versions
- SIMATIC MV540 S (6GF3540-0CD10) toutes versions
- SIMATIC MV550 H (6GF3550-0GE10) toutes versions
- SIMATIC MV550 S (6GF3550-0CD10) toutes versions
- SIMATIC MV560 U (6GF3560-0LE10) toutes versions
- SIMATIC MV560 X (6GF3560-0HE10) toutes versions
- SIMATIC NET PC Software V14 toutes versions
- SIMATIC NET PC Software V15 toutes versions
- SIMATIC NET PC Software V16 toutes versions
- SIMATIC NET PC Software V17 toutes versions
- SIMATIC PCS 7 TeleControl toutes versions
- SIMATIC PCS neo toutes versions
- SIMATIC PDM toutes versions
- SIMATIC RF166C (6GT2002-0EE20) versions antérieures à V2.0.1
- SIMATIC RF185C (6GT2002-0JE10) versions antérieures à V2.0.1
- SIMATIC RF186C (6GT2002-0JE20) versions antérieures à V2.0.1
- SIMATIC RF186CI (6GT2002-0JE50) versions antérieures à V2.0.1
- SIMATIC RF188C (6GT2002-0JE40) versions antérieures à V2.0.1
- SIMATIC RF188CI (6GT2002-0JE60) versions antérieures à V2.0.1
- SIMATIC RF360R (6GT2801-5BA30) versions antérieures à V2.0.1
- SIMATIC RF610R (6GT2811-6BC10) versions antérieures à V4.0.1
- SIMATIC RF615R (6GT2811-6CC10) versions antérieures à V4.0.1
- SIMATIC RF650R (6GT2811-6AB20) versions antérieures à V4.0.1
- SIMATIC RF680R (6GT2811-6AA10) versions antérieures à V4.0.1
- SIMATIC RF685R (6GT2811-6CA10) versions antérieures à V4.0.1
- SIMATIC S7-1200 CPU family (incl. SIPLUS variants) toutes versions
- SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) toutes versions
- SIMATIC S7-1500 Software Controller (incl. F) toutes versions
- SIMATIC S7-PLCSIM Advanced toutes versions
- SIMATIC STEP 7 (TIA Portal) toutes versions
- SIMATIC STEP 7 V5.X toutes versions
- SIMATIC WinCC (TIA Portal) toutes versions
- SINAUT Software ST7sc toutes versions
- SINAUT ST7CC toutes versions
- SINEC INS toutes versions
- SINEC NMS toutes versions
- SINEC NMS toutes versions

- SINEMA Remote Connect Server versions antérieures à V3.1
- SINEMA Remote Connect Server versions antérieures à 3.0 SP2
- SINEMA Remote Connect Server versions antérieures à V3.1
- SINEMA Remote Connect Server versions antérieures à V3.1
- SINEMA Server V14 toutes versions
- SINUMERIK Edge versions antérieures à V3.3.0
- SIPLUS ET 200SP CP 1543SP-1 ISEC (6AG1543-6WX00-7XE0) toutes versions
- SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (6AG2543-6WX00-4XE0) toutes versions
- SIPLUS NET CP 1242-7 V2 (6AG1242-7KX31-7XE0) toutes versions
- SIPLUS NET CP 1543-1 (6AG1543-1AX00-2XE0) toutes versions
- SIPLUS NET CP 343-1 Advanced (6AG1343-1GX31-4XE0) toutes versions
- SIPLUS NET CP 443-1 Advanced (6AG1443-1GX30-4XE0) toutes versions
- SIPLUS S7-1200 CP 1243-1 (6AG1243-1BX30-2AX0) toutes versions
- SIPLUS S7-1200 CP 1243-1 RAIL (6AG2243-1BX30-1XE0) toutes versions
- SIPLUS TIM 1531 IRC (6AG1543-1MX00-7XE0) toutes versions
- Spectrum Power 4 toutes versions using Shared HIS
- Spectrum Power 7 toutes versions using Shared HIS
- Spectrum Power MGMS toutes versions using Shared HIS
- TALON TC Compact (BACnet) versions antérieures à V3.5
- TALON TC Modular (BACnet) versions antérieures à V3.5
- Teamcenter Active Workspace V5.2 versions antérieures à V5.2.9
- Teamcenter Active Workspace V6.0 versions antérieures à V6.0.3
- Teamcenter V12.4 versions antérieures à V12.4.0.13
- Teamcenter V13.0 versions antérieures à V13.0.0.9
- Teamcenter V13.1 versions antérieures à V13.1.0.9
- Teamcenter V13.2 toutes versions
- Teamcenter V13.3 versions antérieures à V13.3.0.3
- Teamcenter V14.0 toutes versions
- TeleControl Server Basic V3 toutes versions
- TIA Administrator toutes versions
- TIA Portal Cloud toutes versions
- TIA Portal V15 toutes versions
- TIA Portal V16 toutes versions
- TIA Portal V17 toutes versions
- TIM 1531 IRC (6GK7543-1MX00-0XE0) toutes versions
- Xpedition Designer versions antérieures à X.2.11

Identificateurs externes

- CVE-2021-40438 CVE-2021-4034 CVE-2022-0847 CVE-2020-9273 CVE-2020-27304 CVE-2021-45960 CVE-2022-22822 CVE-2022-22823 CVE-2022-22824 CVE-2022-22825 CVE-2022-22826 CVE-2022-22827 CVE-2022-23990 CVE-2022-25236 CVE-2022-25315 CVE-2021-39275 CVE-2022-23852 CVE-2022-25235 CVE-2022-0778 CVE-2021-33910

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 14 Juin 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 14 Juin 2022 :

- https://cert-portal.siemens.com/productcert/html/ssa-306654.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: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma