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 systèmes industriels de Siemens
Numéro de Référence	3330121121
Date de Publication	12 Novembre 2021
Risque	Important
Impact	Important

Systèmes affectés

- SIMATIC Information Server toutes versions >= V2019 SP1
- SIMATIC PCS 7 V8.2 toutes versions
- SIMATIC PCS 7 V9.0 toutes versions
- SIMATIC PCS 7 V9.1 toutes versions
- SIMATIC RTLS Locating Manager toutes versions antérieures à V2.12
- SIMATIC WinCC OA V3.17 toutes versions
- SIMATIC WinCC OA V3.18 toutes versions
- SIMATIC WinCC V15 toutes versions
- SIMATIC WinCC V16 toutes versions
- SIMATIC WinCC V17 toutes versions
- SIMATIC WinCC V7.4 toutes versions
- SIMATIC WinCC V7.5 toutes versions antérieures à V7.5 SP2 Update 5
- APOGEE MBC (PPC) (BACnet) toutes versions
- APOGEE MBC (PPC) (P2 Ethernet) toutes versions
- APOGEE MEC (PPC) (BACnet) toutes versions
- APOGEE MEC (PPC) (P2 Ethernet) toutes versions
- APOGEE PXC Compact (BACnet) toutes versions
- APOGEE PXC Compact (P2 Ethernet) toutes versions
- APOGEE PXC Modular (BACnet) toutes versions
- APOGEE PXC Modular (P2 Ethernet) 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

- Capital VSTAR toutes versions
- Capital VSTAR versions incluant les modules DNS
- Climatix POL909 (AWM module) toutes versions antérieures à V11.34
- Mendix Applications using Mendix 7 toutes versions antérieures à V7.23.26
- Mendix Applications using Mendix 8 toutes versions antérieures à V8.18.13
- Mendix Applications using Mendix 9 toutes versions antérieures à V9.6.2
- Nucleus NET toutes versions
- Nucleus ReadyStart V3 toutes versions antérieures à V2012.12
- Nucleus ReadyStart V3 toutes versions antérieures à V2013.08
- Nucleus ReadyStart V3 toutes versions antérieures à V2017.02.4
- Nucleus ReadyStart V4 toutes versions antérieures à V4.1.1
- Nucleus Source Code toutes versions
- Nucleus Source Code versions incluant les modules DNS
- NX 1953 Series toutes versions antérieures à V1973.3700
- NX 1980 Series toutes versions antérieures à V1984
- NX 1980 Series toutes versions antérieures à V1988
- PSS(R)E V34 toutes versions antérieures à V34.9.1
- PSS(R)E V35 toutes versions antérieures à V35.3.2
- PSS(R)ODMS V12 toutes versions antérieures à V12.2.6.1
- SCALANCE W1750D toutes versions antérieures à V8.7.1.3
- SENTRON powermanager V3 toutes versions
- SICAM 230 toutes versions
- Siveillance Video DLNA Server 2019 R1, 2019 R2, 2019 R3
- Siveillance Video DLNA Server 2020 R1, 2020 R2, 2020 R3
- Siveillance Video DLNA Server 2021 R1
- TALON TC Compact (BACnet) toutes versions
- TALON TC Modular (BACnet) toutes versions

Identificateurs externes

- CVE-2021-31344, CVE-2021-31345, CVE-2021-31346, CVE-2021-31881, CVE-2021-31882, CVE-2021-31883, CVE-2021-31884, CVE-2021-31885, CVE-2021-31886, CVE-2021-31887, CVE-2021-31888, CVE-2021-31889, CVE-2021-31890, CVE-2020-10052, CVE-2020-10053, CVE-2020-10054, CVE-2021-41535, CVE-2021-41538, CVE-2021-42015, CVE-2021-37207, CVE-2021-41057, CVE-2021-40366, CVE-2021-41533, CVE-2021-41534, CVE-2021-42021, CVE-2021-42025, CVE-2021-42026, CVE-2021-40358, CVE-2021-40359, CVE-2021-40364, CVE-2021-37727, CVE-2021-37734, CVE-2021-37726, CVE-2021-37730, CVE-2021-37732, CVE-2021-37735, CVE-2020-15795, CVE-2020-27009, CVE-2021-27393, CVE-2021-25663, CVE-2021-

25664, CVE-2020-28388, CVE-2021-25677, CVE-2020-27736, CVE-2020-27737, CVE-2020-27738

Bilan de la vulnérabilité

Plusieurs vulnérabilités ont été corrigées dans les systèmes industriels de Siemens susmentionnés. Un attaquant pourrait exploiter ces failles afin de réussir une exécution de code arbitraire à distance, un déni de service ou un contournement de la politique de sécurité.

Solution

Veuillez se référer au bulletin de sécurité Siemens du 09 Novembre 2021 afin d'installer les nouvelles mises à jour.

Risque

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

Référence

Bulletin de sécurité Siemens du 09 Novembre 2021 :

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

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