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	41821105/23
Date de Publication	11 Mai 2023
Risque	Important
Impact	Important

Systèmes affectés

- SCALANCE LPE9403 (6GK5998-3GS00-2AC2) versions antérieures à V2.1
- SIMATIC Cloud Connect 7 CC712 (6GK1411-1AC00) versions V2.x versions antérieures à V2.1
- SIMATIC Cloud Connect 7 CC716 (6GK1411-5AC00) versions V2.x versions antérieures à V2.1
- SINEC NMS versions antérieures à V1.0.3.1
- Siveillance Video 2020 R2 versions antérieures à V20.2 HotfixRev14
- Siveillance Video 2020 R3 versions antérieures à V20.3 HotfixRev12
- Siveillance Video 2021 R1 versions antérieures à V21.1 HotfixRev12
- Siveillance Video 2021 R2 versions antérieures à V21.2 HotfixRev8
- Siveillance Video 2022 R1 versions antérieures à V22.1 HotfixRev7
- Siveillance Video 2022 R2 versions antérieures à V22.2 HotfixRev5
- Siveillance Video 2022 R3 versions antérieures à V22.3 HotfixRev2
- Siveillance Video 2023 R1 versions antérieures à V23.1 HotfixRev1
- Solid Edge SE2023 versions antérieures à VX.223.0 Update 3
- SIMATIC S7-400 CPU 414-3 PN/DP V7 (6ES7414-3EM07-0AB0) versions antérieures à V7.0.3
- SIMATIC S7-400 CPU 414F-3 PN/DP V7 (6ES7414-3FM07-0AB0) versions antérieures à V7.0.3
- SIMATIC S7-400 CPU 416-3 PN/DP V7 (6ES7416-3ES07-0AB0) versions antérieures à V7.0.3

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

- SIMATIC S7-400 CPU 416F-3 PN/DP V7 (6ES7416-3FS07-0AB0) versions antérieures à V7.0.3
- SIMATIC S7-400 CPU 412-2 PN V7 (6ES7412-2EK07-0AB0) versions antérieures à V7.0.3
- SCALANCE W1750D (JP) (6GK5750-2HX01-1AD0) toutes versions
- SCALANCE W1750D (ROW) (6GK5750-2HX01-1AA0) toutes versions
- SCALANCE W1750D (USA) (6GK5750-2HX01-1AB0) toutes versions

Identificateurs externes

- CVE-2022-32221 , CVE-2022-35252 , CVE-2022-35260 , CVE-2022-40674 , CVE-2022-42915 , CVE-2022-42916 , CVE-2022-43551 , CVE-2022-43552 , CVE-2022-43680 , CVE-2022-47522 , CVE-2023-0973 , CVE-2023-27407 , CVE-2023-27408 , CVE-2023-27409 , CVE-2023-27410 , CVE-2023-28832 , CVE-2023-29103 , CVE-2023-29104 , CVE-2023-29105 , CVE-2023-29106 , CVE-2023-29107 , CVE-2023-29128 , CVE-2023-30898 , CVE-2023-30899 , CVE-2023-30985 , CVE-2023-30986 , CVE-2019-10936

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 09 Mai 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

Bulletins de sécurité Siemens du 09 Mai 2023:

- https://cert-portal.siemens.com/productcert/html/ssa-932528.html
- https://cert-portal.siemens.com/productcert/html/ssa-789345.html
- https://cert-portal.siemens.com/productcert/html/ssa-555292.html
- https://cert-portal.siemens.com/productcert/html/ssa-325383.html
- https://cert-portal.siemens.com/productcert/html/ssa-516174.html
- https://cert-portal.siemens.com/productcert/html/ssa-892048.html

- https://cert-portal.siemens.com/productcert/html/ssa-473245.html