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 critiques dans les produits Siemens
Numéro de Référence	62011303/26
Date de Publication	13 Mars 2026
Risque	Critique
Impact	Critique

Systèmes affectés

- SIMATIC S7-1500 versions antérieures à 4.1.2
- SIMATIC S7-1500 toutes versions pour la vulnérabilité CVE-2025-40943
- SIMATIC ET 200SP Open Controller CPU 1515SP PC3 (incl. SIPLUS variants) V3 CPUs - Windows OS toutes versions pour la vulnérabilité CVE-2025-40943
- SIMATIC ET 200SP Open Controller CPU 1515SP PC3 (incl. SIPLUS variants) V3 CPUs - Industrial OS toutes versions pour la vulnérabilité CVE-2025-40943
- SIMATIC ET 200SP Open Controller CPU 1515SP PC3 (incl. SIPLUS variants) V2 CPUs - Windows OS toutes versions pour la vulnérabilité CVE-2025-40943
- SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) V3 CPUs - Windows OS toutes versions pour la vulnérabilité CVE-2025-40943
- SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) V3 CPUs - Industrial OS toutes versions pour la vulnérabilité CVE-2025-40943
- SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) V2 CPUs - Windows OS toutes versions pour la vulnérabilité CVE-2025-40943
- SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) toutes versions pour la vulnérabilité CVE-2025-40943
- SIMATIC ET 200SP CPU 1514SPT-2 PN (6ES7514-2VN03-0AB0) versions antérieures à 4.1.2
- SIMATIC ET 200SP CPU 1514SPT F-2 PN (6ES7514-2WN03-0AB0) versions antérieures à 4.1.2
- SIMATIC ET 200SP CPU 1514SP-2 PN (6ES7514-2DN03-0AB0) versions antérieures à 4.1.2
- SIMATIC ET 200SP CPU 1514SP F-2 PN (6ES7514-2SN03-0AB0) versions antérieures à 4.1.2

- SIMATIC ET 200SP CPU 1512SP-1 PN (6ES7512-1DM03-0AB0) versions antérieures à 4.1.2
- SIMATIC ET 200SP CPU 1512SP-1 PN (6ES7512-1DK01-0AB0) toutes versions pour la vulnérabilité CVE-2025-40943
- SIMATIC ET 200SP CPU 1512SP F-1 PN (6ES7512-1SM03-0AB0) versions antérieures à 4.1.2
- SIMATIC ET 200SP CPU 1512SP F-1 PN (6ES7512-1SK01-0AB0) toutes versions pour la vulnérabilité CVE-2025-40943
- SIMATIC ET 200SP CPU 1510SP-1 PN (6ES7510-1DK03-0AB0) versions antérieures à 4.1.2
- SIMATIC ET 200SP CPU 1510SP-1 PN (6ES7510-1DJ01-0AB0) toutes versions pour la vulnérabilité CVE-2025-40943
- SIMATIC ET 200SP CPU 1510SP F-1 PN (6ES7510-1SK03-0AB0) versions antérieures à 4.1.2
- SIMATIC ET 200SP CPU 1510SP F-1 PN (6ES7510-1SJ01-0AB0) toutes versions pour la vulnérabilité CVE-2025-40943
- SIMATIC Drive Controller CPU 1507D TF (6ES7615-7DF10-0AB0) toutes versions pour la vulnérabilité CVE-2025-40943
- SIMATIC Drive Controller CPU 1504D TF (6ES7615-4DF10-0AB0) toutes versions pour la vulnérabilité CVE-2025-40943
- SICAM SIAPP SDK versions antérieures à 2.1.7

Identificateurs externes

- CVE-2025-40943 CVE-2026-25569 CVE-2026-25570 CVE-2026-25571
- CVE-2026-25572 CVE-2026-25573 CVE-2026-25605

Bilan de la vulnérabilité

Plusieurs vulnérabilités critiques ont été corrigées dans les systèmes industriels de Siemens susmentionnés. L'exploitation de ces failles pourrait permettre à un attaquant distant non authentifié de contourner l'authentification et de se faire passer pour un utilisateur légitime, de causer un déni de service et de contourner la politique de sécurité.

Solution

Veuillez se référer au bulletin de sécurité Siemens du 10 Mars 2026 pour plus d'information.

Risque

- Déni de service ;
- Contournement de la politique de sécurité ;
- Elévation de privilèges ;
- Atteinte à la confidentialité des données ;

Annexe

Bulletin de sécurité Siemens du 10 Mars 2026:

- https://www.siemens.com/en-us/content/cert-services/?d=2026-03#SiemensSecurityAdvisories

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