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	58421211/25
Date de Publication	12 Novembre 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- Altair Grid Engine versions avant V2025.1.0
- COMOS versions avant V10.4.5
- Fortigate NGFW sur RUGGEDCOM APE1808 versions avant 7.4.7
- LOGO! 8 BM Devices
- Mendix OIDC SSO Module
- Les produits SIMATIC utilisant OPC UA
- RUGGEDCOM ROX II
- SICAM GridEdge versions avant V2.7.3 et V2.6.6
- SICAM P850 / P855 versions avant V3.11
- SIMATIC IPCs, SIMATIC Tablet PCs, SIMATIC Field PGs (EFI variable)
- SIPROTEC 5
- Siemens Software Center
- Solid Edge
- Spectrum Power 4 versions antérieures à v4.70 SP12 Security Patch 2
- Web Installer utilisé par Online Software Delivery (OSD)

Identificateurs externes

- CVE-2025-58903 CVE-2025-58325 CVE-2025-57740 CVE-2025-54822
- CVE-2025-53744 CVE-2025-47890 CVE-2025-47295 CVE-2025-40827
- CVE-2025-40817 CVE-2025-40816 CVE-2025-40815 CVE-2025-40763
- CVE-2025-40760 CVE-2025-40591 CVE-2025-40571 CVE-2025-33025
- CVE-2025-33024 CVE-2025-32469 CVE-2025-31514 CVE-2025-31366
- CVE-2025-30033 CVE-2025-25253 CVE-2025-25252 CVE-2025-25250

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

- CVE-2025-25248 CVE-2025-24471 CVE-2025-22862 CVE-2025-22258
- CVE-2025-22254 CVE-2025-22252 CVE-2025-22251 CVE-2024-56182
- CVE-2024-56181 CVE-2024-55599 CVE-2024-54021 CVE-2024-53649
- CVE-2024-53648 CVE-2024-52965 CVE-2024-52963 CVE-2024-50571
- CVE-2024-50568 CVE-2024-50565 CVE-2024-50563 CVE-2024-50562
- CVE-2024-48886 CVE-2024-48885 CVE-2024-48884 CVE-2024-47569
- CVE-2024-46670 CVE-2024-46669 CVE-2024-46668 CVE-2024-46666
- CVE-2024-46665 CVE-2024-45324 CVE-2024-40591 CVE-2024-38867
- CVE-2024-36505 CVE-2024-36504 CVE-2024-3596 CVE-2024-35279
- CVE-2024-33510 CVE-2024-32122 CVE-2024-32014 CVE-2024-32011
- CVE-2024-32010 CVE-2024-32009 CVE-2024-32008 CVE-2024-26015
- CVE-2024-26013 CVE-2024-26011 CVE-2024-26010 CVE-2024-26008
- CVE-2024-26007 CVE-2024-26006 CVE-2024-23662 CVE-2024-23113
- CVE-2024-23112 CVE-2024-23111 CVE-2024-23110 CVE-2024-21762
- CVE-2024-21754 CVE-2024-0056 CVE-2023-50176 CVE-2023-48784
- CVE-2023-47537 CVE-2023-46720 CVE-2023-46718 CVE-2023-46717
- CVE-2023-46715 CVE-2023-46714 CVE-2023-45586 CVE-2023-45583
- CVE-2023-45133 CVE-2023-44487 CVE-2023-44250 CVE-2023-44247
- CVE-2023-42790 CVE-2023-42789 CVE-2023-42786 CVE-2023-42785
- CVE-2023-41677 CVE-2023-40721 CVE-2023-38546 CVE-2023-38545
- CVE-2023-36640 CVE-2023-31238 CVE-2023-30901 CVE-2023-28831
- CVE-2023-28766 CVE-2023-27997 CVE-2022-45862 CVE-2022-45044
- CVE-2022-42475 CVE-2022-34464 CVE-2022-30231 CVE-2022-30230
- CVE-2022-30229 CVE-2022-30228 CVE-2022-23439

Bilan de la vulnérabilité

Plusieurs vulnérabilités critiques ont été corrigées dans les systèmes industriels de Siemens susmentionnés. Un attaquant pourrait exploiter ces failles afin de causer un déni de service, contourner la politique de sécurité, réussir une élévation de privilèges, exécuter du code arbitraire à distance, porter atteinte à la confidentialité des données et réussir des injections SQL .

Solution

Veuillez se référer au bulletin de sécurité Siemens du 11 Novembre 2025 pour plus d'information.

Risque

- Déni de service
- Contournement de la politique de sécurité
- Injection SQL
- Elévation de privilèges
- Exécution du code arbitraire à distance
- Atteinte à la confidentialité des données

Annexe

Bulletin de sécurité Siemens du 11 Novembre 2025:

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