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	Vulnérabilité dans les produits industriels de Schneider Electric
Numéro de Référence	43811511/23
Date de Publication	15 Novembre 2023
Risque	Important
Impact	Important

Systèmes affectés

- Schneider Electric Advanced Reporting and Dashboards Module for EcoStruxure Power Operation versions 2020 antérieures à 2020 CU3
- Schneider Electric Advanced Reporting and Dashboards Module for EcoStruxure Power Operation versions 2021 antérieures à 2021 CU2
- Schneider Electric Advanced Reporting and Dashboards Module for EcoStruxure Power SCADA Operation (PSO) versions 2020 antérieures à 2020 CU3
- Schneider Electric EcoStruxure Power Monitoring Expert (PME) versions 2020 antérieures à 2020 CU3
- Schneider Electric EcoStruxure Power Monitoring Expert (PME) versions 2021 antérieures à 2021 CU2
- Schneider Electric Galaxy VS version 6.82
- Schneider Electric Galaxy VL version 12.21
- PowerLogic ION8650 toutes versions sans le dernier correctif de sécurité
- PowerLogic ION8800 toutes versions sans le dernier correctif de sécurité

Identificateurs externes

- CVE-2023-5984 CVE-2023-5985 CVE-2023-5986 CVE-2023-5987 CVE-2023-6032

Bilan de la vulnérabilité

Plusieurs vulnérabilités ont été corrigées dans les produits industriels susmentionnés de Schneider Electric. L'exploitation de ces failles permet à un attaquant d'injecter de code indirecte à distance (XSS), de contourner la politique de sécurité et de porter atteinte à la confidentialité des données.

Solution

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

Veuillez se référer au bulletin de sécurité Schneider Electric 14 novembre 2023, afin d'installer les dernières mises à jour.

Risque

- Atteinte à la confidentialité des données
- Contournement de la politique de sécurité
- Injection de code indirecte à distance (XSS)

Références

Bulletin de sécurité Schneider Electric du 14 novembre 2023:

- https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-318-01&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-318-01.pdf
- https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-318-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-318-02.pdf
- https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-318-03&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-318-03.pdf