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 Schneider Electric
Numéro de Référence	41841105/23
Date de Publication	11 Mai 2023
Risque	Important
Impact	Important

Systèmes affectés

- Altivar 32/320 et Lexium 32 Ethernet TCP/IP communication module (VW3A3616) versions antérieures à V1.20IE01
- EcoStruxure Power Operation versions 2021 antérieures à 2021 CU3
- EcoStruxure Power Operation versions 2022 antérieures à 2022 CU1
- EcoStruxure Power SCADA Operation versions 2020 R2
- Modicon X80 Module (part number BMXNOM0200) versions antérieures à V1.60
- OPC Factory Server (OFS) versions antérieures à V3.63SP2
- Power SCADA Anywhere versions 1.1 et 1.2 antérieures à Plant SCADA Anywhere version 2023
- PowerLogic ION7400 antérieures à 4.0.0 sans le dernier correctif de sécurité
- PowerLogic ION8650 toutes versions
- PowerLogic ION8800 toutes versions
- PowerLogic ION9000 antérieures à 4.0.0 sans le dernier correctif de sécurité
- PowerLogic PM8000 antérieures à 4.0.0 sans le dernier correctif de sécurité
- Produits Legacy ION toutes versions

Identificateurs externes

- CVE-2023-2161 , CVE-2022-46680 , CVE-2021-31400 , CVE-2021-31401 , CVE-2020-35683 , CVE-2020-35684 , CVE-2020-35685 , CVE-2023-1256 , CVE-2020-35198 , CVE-2020-28895 , CVE-2021-3711 , CVE-2022-23854 , CVE-2020-11022

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

Bilan de la vulnérabilité

Plusieurs vulnérabilités critiques ont été corrigées dans les produits industriels susmentionnés de Schneider Electric. L'exploitation de ces failles permet à un attaquant de causer un déni de service, de réussir une élévation de privilèges et potentiellement réussir une exécution de code à distance.

Solution

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

Risque

- Exécution du code arbitraire
- Elévation de privilèges
- Déni de service

Références

Bulletin de sécurité Schneider Electric du 09 Mai 2023:

- https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-129-01&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-129-01.pdf
- https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-129-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-129-02.pdf
- https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-129-03&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-129-03.pdf
- https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-129-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-129-04.pdf
- https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-217-01&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2021-217-01_NicheStack_Security_Notification.pdf
- https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-313-05&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2021-313-05_BadAlloc_Vulnerabilities_Security_Notification.pdf