



BULLETIN DE SECURITE

Titre	Vulnérabilités critiques dans les produits industriels de Schneider Electric
Numéro de Référence	58431211/25
Date de Publication	12 Novembre 2025
Risque	Critique
Impact	Critique

Systemes affectés

- PowerChute™ Serial Shutdown (versions v1.3 et antérieures)
- EcoStruxure™ Machine SCADA Expert (versions antérieures à 2023.1 Patch 1)
- Pro-face BLUE Open Studio (versions antérieures à 2023.1 Patch 1)
- Produits basés sur CODESYS Runtime :
 - Easy Harmony HMIET6 / HMIFT6
 - Easy Modicon M310, M218, M241, M251, M258, M262
 - HMISCU Controller
 - Harmony (Magelis) HMIGK/HMIGTO/HMIGTU/HMIGTUX/HMISTU, iPC séries
 - PacDrive 3 Controllers (LMC Eco/Pro/Pro2)
 - EcoStruxure™ Machine Expert, Vijeo Designer intégré
- Saitel DR & DP Remote Terminal Units (versions DR ≤ 11.06.29, DP ≤ 11.06.34)
- EcoStruxure™ Power Monitoring Expert (PME) (versions 2022 à 2024 R2)
- EcoStruxure™ Power Operation (EPO) / Power SCADA Operation (PSO)
- EcoStruxure™ Control Expert, Process Expert, OPC UA Server Expert, Operator Terminal Expert, Architecture Builder, Zelio Soft 2, Machine Expert Twin, et Pro-face BLUE utilisant FlexNet Publisher.

Identificateurs externes

- CVE-2025-11565 CVE-2025-11566 CVE-2025-11567 CVE-2025-54923
- CVE-2025-54924 CVE-2025-54925 CVE-2025-54926 CVE-2025-54927
- CVE-2025-8453

Bilan de la vulnérabilité

Plusieurs vulnérabilités critiques ont été corrigées dans les produits industriels de Schneider Electric. L'exploitation de ces failles pourrait entraîner l'exécution de code à distance, la perte de confidentialité, le contournement de l'authentification, de réussir une élévation de

privilèges ou encore l'accès non autorisé à des ressources sensibles.

Solution

Veillez se référer au bulletin de sécurité Schneider Electric 11 Novembre 2025, afin d'installer les dernières mises à jour.

Risque

- Accès aux informations confidentielles
- Contournement de la politique de sécurité
- Atteinte à la confidentialité des données
- Exécution du code arbitraire à distance
- Élévation de privilèges

Références

Bulletin de sécurité Schneider Electric du 11 Novembre 2025:

- https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2025-315-01&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2025-315-01.pdf
- https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2025-315-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2025-315-02.pdf
- https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-192-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-192-04.pdf
- https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2025-224-01&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2025-224-01.pdf
- https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2025-224-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2025-224-02.pdf
- https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2025-014-07&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2025-014-07.pdf