



BULLETIN DE SECURITE

Titre	Vulnérabilités dans les produits SCADA de Siemens
Numéro de Référence	56631009/25
Date de Publication	10 Septembre 2025
Risque	Important
Impact	Important

Systemes affectés

- SIMATIC Virtualization as a Service (SIVaaS)
- SIMATIC Technology Package TPCamGen (6ES7823-0FE30-1AA0)
- SIMATIC S7-1500 TM MFP - GNU/Linux
- SIMATIC S7-1500 TM MFP - BIOS
- SIMOTION OA MIIF (6AU1820-3DA20-0AB0)
- SIMOTION OACAMGEN (6AU1820-3EA20-0AB0)
- SIMOTION OALECO (6AU1820-3HA20-0AB0)
- SIMOTION OAVIBX (6AU1820-3CA20-0AB0)
- OpenPCS 7
- Automation License Manager
- Industrial Edge - OPC UA Connector
- Industrial Edge - SIMATIC S7 Connector App versions antérieures à V1.7
- Industrial Edge Management OS (IEM-OS)
- SIMATIC PCS neo V5.0
- SIMATIC PCS neo V4.1
- User Management Component (UMC) toutes les versions antérieures à V2.15.1.3
- RUGGEDCOM APE1808 Toutes les versions avec Fortinet NGFW avant V7.4.1

Identificateurs externes

- CVE-2025-40795 CVE-2025-40796 CVE-2025-40797
- CVE-2025-40798 CVE-2025-40804 CVE-2025-43715

Bilan de la vulnérabilité

Plusieurs vulnérabilités ont été corrigées dans les produits SCADA de Siemens. L'exploitation de ces failles pourrait permettre à un attaquant distant de réussir un contournement d'authentification, de porter atteinte à la confidentialité et l'intégrité des données, de causer un déni de service, d'exécuter du code arbitraire à distance et de gagner une élévation de privilèges.

Solution

Veuillez se référer au bulletin de sécurité Siemens du 09 Septembre 2025 pour plus d'information.

Risque

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

Annexe

Bulletin de sécurité Siemens du 09 Septembre 2025:

- <https://cert-portal.siemens.com/productcert/html/ssa-534283.html>
- <https://cert-portal.siemens.com/productcert/html/ssa-265688.html>
- <https://cert-portal.siemens.com/productcert/html/ssa-563922.html>
- <https://cert-portal.siemens.com/productcert/html/ssa-691715.html>
- <https://cert-portal.siemens.com/productcert/html/ssa-503939.html>
- <https://cert-portal.siemens.com/productcert/html/ssa-282044.html>
- <https://cert-portal.siemens.com/productcert/html/ssa-712929.html>
- <https://cert-portal.siemens.com/productcert/html/ssa-640476.html>
- <https://cert-portal.siemens.com/productcert/html/ssa-864900.html>

- <https://cert-portal.siemens.com/productcert/html/ssa-027652.html>
- <https://cert-portal.siemens.com/productcert/html/ssa-916339.html>
- <https://cert-portal.siemens.com/productcert/html/ssa-494539.html>