



BULLETIN DE SECURITE

Titre	Vulnérabilités dans les produits Siemens
Numéro de Référence	54511505/25
Date de Publication	15 Mai 2025
Risque	Critique
Impact	Critique

Systemes affectés

- CPCI85 Central Processing/Communication toutes versions
- Desigo CC toutes versions
- POWER METER SICAM Q100 family versions antérieures à V2.70
- POWER METER SICAM Q200 family toutes versions
- SCALANCE LPE9403 toutes versions
- SICAM GridPass versions antérieures à V2.50
- SICORE Base system toutes versions
- SIMATIC IPC RS-828A toutes versions
- SIMATIC PCS neo V4.1 toutes versions – pas de correctif prévu
- SIMATIC PCS neo V5.0 toutes versions
- SIMATIC PCS neo versions antérieures à V4.1 Update 3
- SIMATIC PCS neo versions antérieures à V5.0 Update 1
- SIPROTEC 5 6MD84 CP300 toutes versions
- SIPROTEC 5 6MD85 CP300 versions antérieures à V7.80
- SIPROTEC 5 6MD86 CP300 versions antérieures à V7.80
- SIPROTEC 5 6MD89 CP300 V9.6 versions antérieures à V9.68
- SIPROTEC 5 6MD89 CP300 versions antérieures à V7.80
- SIPROTEC 5 6MU85 CP300 toutes versions
- SIPROTEC 5 7KE85 CP300 versions antérieures à V7.80
- SIPROTEC 5 7SA86 CP300 versions antérieures à V7.80

- SIPROTEC 5 7SA87 CP300 versions antérieures à V7.80
- SIPROTEC 5 7SD86 CP300 versions antérieures à V7.80
- SIPROTEC 5 7SD87 CP300 versions antérieures à V7.80
- SIPROTEC 5 7SJ85 CP300 versions antérieures à V7.80
- SIPROTEC 5 7SJ86 CP300 versions antérieures à V7.80
- SIPROTEC 5 7SK85 CP300 versions antérieures à V7.80
- SIPROTEC 5 7SL86 CP300 versions antérieures à V7.80
- SIPROTEC 5 7SL87 CP300 versions antérieures à V7.80
- SIPROTEC 5 7SS85 CP300 versions antérieures à V7.80
- SIPROTEC 5 7ST85 CP300 versions antérieures à V9.68
- SIPROTEC 5 7ST86 CP300 versions antérieures à V9.83
- SIPROTEC 5 7SX85 CP300 toutes versions
- SIPROTEC 5 7UM85 CP300 versions antérieures à V7.80
- SIPROTEC 5 7UT85 CP300 versions antérieures à V7.80
- SIPROTEC 5 7UT86 CP300 versions antérieures à V7.80
- SIPROTEC 5 7UT87 CP300 versions antérieures à V7.80
- SIPROTEC 5 7VE85 CP300 versions antérieures à V7.80
- SIPROTEC 5 7VK87 CP300 versions antérieures à V7.80
- SIPROTEC 5 7VU85 CP300 toutes versions
- Totally Integrated Automation Portal TIA Portal V17 toutes versions
- Totally Integrated Automation Portal TIA Portal V18 toutes versions
- Totally Integrated Automation Portal TIA Portal V19 toutes versions
- Totally Integrated Automation Portal TIA Portal V20 toutes versions

Identificateurs externes

- CVE-2024-23815 CVE-2024-3596 CVE-2024-54085
- CVE-2025-30174 CVE-2025-30175 CVE-2025-30176
- CVE-2025-40566 CVE-2025-40572 CVE-2025-40573
- CVE-2025-40574 CVE-2025-40575 CVE-2025-40576
- CVE-2025-40577 CVE-2025-40578 CVE-2025-40579
- CVE-2025-40580 CVE-2025-40581 CVE-2025-40582
- CVE-2025-40583

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, exécuter du code arbitraire à distance, porter atteinte à la confidentialité des données et réussir des injections SQL .

Solution

Veillez se référer au bulletin de sécurité Siemens du 13 Mai 2025 pour plus d'information.

Risque

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

Annexe

Bulletin de sécurité Siemens du 13 Mai 2025:

- <https://cert-portal.siemens.com/productcert/html/ssa-327438.html>
- <https://cert-portal.siemens.com/productcert/html/ssa-339086.html>
- <https://cert-portal.siemens.com/productcert/html/ssa-446307.html>
- <https://cert-portal.siemens.com/productcert/html/ssa-523418.html>
- <https://cert-portal.siemens.com/productcert/html/ssa-614723.html>
- <https://cert-portal.siemens.com/productcert/html/ssa-794185.html>