DJ-CERT
Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 15-05-2024

BULLETIN ALERTES

Object	Multiples Vulnérabilités dans les produits Siemens
Réference	1140
Date de Publication	2024-05-14
Sévérité	Critique

IMPACT :

- Atteinte à la confidentialité des données
- Contournement de la politique de sécurité
- Déni de service
- Exécution de code arbitraire à distance
- Élévation de privilèges

SYSTÉME AFFECTÉ :

- S7-PCT toutes versions
- Sicam CPCI85 Central Processing/Communication versions antérieures à V5.30
- Sicam OPUPI0 AMQP/MQTT versions antérieures à V5.30
- Sicam SICORE Base system versions antérieures à V1.3.0
- Sicam CPC80 Central Processing/Communication versions antérieures à V16.41
- SIMATIC Automation Tool toutes versions
- SIMATIC BATCH V9.1 toutes versions
- SIMATIC CN 4100 versions antérieures à V3.0
- SIMATIC NET PC Software toutes versions
- SIMATIC PCS 7 V9.1 toutes versions
- SIMATIC PDM V9.2 toutes versions
- SIMATIC Route Control V9.1 toutes versions
- SIMATIC STEP 7 V5 toutes versions
- SIMATIC WinCC OA V3.17 toutes versions. L'éditeur indique que le produit ne bénéficiera pas de correctif de sécurité pour la vulnérabilité CVE-2023-46280.
- SIMATIC WinCC OA V3.18 versions antérieures à V3.18 P025
- SIMATIC WinCC OA V3.19 versions antérieures à V3.19 P010
- SIMATIC WinCC Runtime Advanced toutes versions
- SIMATIC WinCC Runtime Professional V16 toutes versions
- SIMATIC WinCC Runtime Professional V17 toutes versions
- SIMATIC WinCC Runtime Professional V18 toutes versions
- SIMATIC WinCC Runtime Professional V19 toutes versions
- SIMATIC WinCC Unified PC Runtime toutes versions
- SIMATIC WinCC V7.4 toutes versions. L'éditeur indique que le produit ne bénéficiera pas de correctif de sécurité pour la vulnérabilité CVE-2023-46280.
- SIMATIC WinCC V7.5 toutes versions
- SIMATIC WinCC V8.0 toutes versions
- TIA Portal Cloud Connector versions antérieures à V2.0
- Totally Integrated Automation Portal (TIA Portal) V15.1 toutes versions. L'éditeur indique que le produit ne bénéficiera pas de correctif de sécurité pour la vulnérabilité CVE-2023-46280.
- Totally Integrated Automation Portal (TIA Portal) V16 toutes versions. L'éditeur indique que le produit ne bénéficiera pas de correctif de sécurité pour la vulnérabilité CVE-2023-46280.
- 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 versions antérieures à V19 Update 2

DÉSCRIPTION :

Des nombreuses vulnérabilités ont été découvertes dans les produits Siemens susmentionné.

Ces vulnérabilités permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une élévation de privilèges et une atteinte à la confidentialité des données.

SOLUTION :

Mettre à jour vos produits Siemens. (se réfère à la documentation)

DOCUMENTATION :

- Bulletin de sécurité Siemens SSA-962515 14/05/2024
  https://cert-portal.siemens.com/productcert/html/ssa-962515.html
- Bulletin de sécurité Siemens SSA-871704 14/05/2024
  https://cert-portal.siemens.com/productcert/html/ssa-871704.html
- Bulletin de sécurité Siemens SSA-273900 14/05/2024
  https://cert-portal.siemens.com/productcert/html/ssa-273900.html
- CVE-2023-46280
  https://www.cve.org/CVERecord?id=CVE-2023-46280
- CVE-2024-31484
  https://www.cve.org/CVERecord?id=CVE-2024-31484
- CVE-2024-31485
  https://www.cve.org/CVERecord?id=CVE-2024-31485
- CVE-2024-31486
  https://www.cve.org/CVERecord?id=CVE-2024-31486
- CVE-2024-32740
  https://www.cve.org/CVERecord?id=CVE-2024-32740
- CVE-2024-32741
  https://www.cve.org/CVERecord?id=CVE-2024-32741
- CVE-2024-32742
  https://www.cve.org/CVERecord?id=CVE-2024-32742