Bulletin de sécurité du maCERT

Titre: Vulnérabilités dans les produits Siemens

Numéro de Référence : 20521505/19
Risque : Important
Impact : Important

Systèmes affectés

- SCALANCE W1750D versions antérieures à V8.4.0.1
- SINAMICS PERFECT HARMONY GH180
- SIMATIC PCS 7
- SIMATIC WinCC V7.5 versions antérieures à V7.5 Upd3
- SIMATIC HMI Comfort Panels 4" - 22" versions antérieures à V15.1 Update 1
- SIMATIC HMI Comfort Outdoor Panels 7" & 15" versions antérieures à V15.1 Update 1
- SIMATIC HMI KTP Mobile Panels KTP400F,KTP700, KTP700F, KTP900 et KTP900F versions antérieures à V15.1 Update 1
- SIMATIC WinCC Runtime Advanced versions antérieures à V15.1 Update 1
- SIMATIC WinCC Runtime Professional versions antérieures à V15.1 Update 1
- SIMATIC WinCC (TIA Portal) versions antérieures à V15.1 Update 1
- SIMATIC HMI Classic Devices (TP/MP/OP/MPMobile Panel)
- SISHIP EMCS
- SISHIP IMAC
- SISHIP IPMS

Identificateurs externes

- CVE-2018-7084 CVE-2018-7083 CVE-2018-16417 CVE-2018-7082 CVE-2018-7064 CVE-2019-6578 CVE-2019-6574 CVE-2019-10916 CVE-2019-10917 CVE-2019-10918 CVE-2019-6572 CVE-2019-6576 CVE-2019-6577 CVE-2018-3989 CVE-2018-3990 CVE-2018-3991 CVE-2019-10924 CVE-2019-10919 CVE-2019-10920 CVE-2019-10921 CVE-2019-10922

Bilan de la vulnérabilité

Plusieurs vulnérabilités ont été corrigées dans plusieurs produits Siemens. Un attaquant pourrait exploiter ces failles pour porter atteinte à la confidentialité des données, provoquer un déni de service à distance et réussir une élévation de privilèges.

Solution

Veuillez-vous référer aux bulletins de sécurité Siemens du 14 Mai 2019 afin d'installer les dernières mises à jours :

https://cert-portal.siemens.com/productcert/pdf/ssa-549547.pdf

https://cert-portal.siemens.com/productcert/pdf/ssa-606525.pdf

https://cert-portal.siemens.com/productcert/pdf/ssa-865156.pdf

https://cert-portal.siemens.com/productcert/pdf/ssa-697412.pdf

https://cert-portal.siemens.com/productcert/pdf/ssa-804486.pdf

https://cert-portal.siemens.com/productcert/pdf/ssa-902727.pdf

https://cert-portal.siemens.com/productcert/pdf/ssa-102144.pdf

https://cert-portal.siemens.com/productcert/pdf/ssa-542701.pdf

https://cert-portal.siemens.com/productcert/pdf/ssa-705517.pdf

Risque :

- Porter atteinte à la confidentialité des données ;
- Déni de service à distance ;
- Élévation de privilèges.

Annexe

Bulletins de sécurité Siemens du 14 Mai 2019 :

https://cert-portal.siemens.com/productcert/pdf/ssa-549547.pdf

https://cert-portal.siemens.com/productcert/pdf/ssa-606525.pdf

https://cert-portal.siemens.com/productcert/pdf/ssa-865156.pdf

https://cert-portal.siemens.com/productcert/pdf/ssa-697412.pdf

https://cert-portal.siemens.com/productcert/pdf/ssa-804486.pdf

https://cert-portal.siemens.com/productcert/pdf/ssa-902727.pdf

https://cert-portal.siemens.com/productcert/pdf/ssa-102144.pdf

https://cert-portal.siemens.com/productcert/pdf/ssa-542701.pdf

https://cert-portal.siemens.com/productcert/pdf/ssa-705517.pdf

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: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma