ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Vulnérabilités dans les produits SCADA de SIEMENS
Numéro de Référence	25971607/20
Date de Publication	16 juillet 2020
Risque	Important
Impact	Important

Systèmes affectés

- Opcenter Execution Discrete versions antérieures à v3.2
- Opcenter Execution Foundation versions antérieures à v3.2
- Opcenter Execution Process versions antérieures à v3.2
- Opcenter Execution Core versions antérieures à v8.2
- Opcenter Intelligence
- Opcenter Quality versions antérieures à 11.3
- Opcenter RD&L versions antérieures à 8.1
- Camstar Enterprise Platform : une migration vers Opcenter Execution Core 8.2 est requise
- SIMATIC IT LMS, Production Suite, Notifier Server for Windows, PCS neo
- SIMATIC STEP 7 (TIA Portal) v15
- SIMATIC STEP 7 (TIA Portal) v16 versions antérieures à V16 update 2
- SIMOCODE ES et Soft Starter ES
- SPPA-T3000 Application Server et Terminal Server
- SPPA-T3000 APC UPS avec carte NMC AP9630 ou AP9631
- SIMATIC S7-200 SMART CPU versions antérieures à V2.5.1
- LOGO! 8 BM (incl. variantes SIPLUS) versions antérieures à V1.81.04
- LOGO! 8 BM (incl. variantes SIPLUS) versions antérieures à V1.82.03
- LOGO! 8 BM (incl. variantes SIPLUS) versions antérieures à V1.82.04
- SIMATIC S7-300 CPU (incl. variantes ET200CPUs et SIPLUS) versions antérieures à V3.X.17
- SIMATIC TDC CP51M1 versions antérieures à V1.1.8
- SIMATIC TDC CPU555 versions antérieures à V1.1.1
- SINUMERIK 840D sl versions antérieures à V4.8.6
- SINUMERIK 840D sl versions antérieures à V4.94
- SIMATIC HMI Basic Panels première et seconde génération, Comfort Panels, Mobile

Panels de seconde génération (incl. variantes SIPLUS)
- SIMATIC HMI KTP700F Mobile Arctic
- SIMATIC WinCC Runtime Advanced
- SICAM MMU versions antérieures à V2.05
- SICAM SGU
- SICAM T versions antérieures à V2.18

Identificateurs externes

- CVE-2020-7581 CVE-2020-7587 CVE-2020-7588 CVE-2020-11896 CVE-2020-0545
- CVE-2020-7576 CVE-2020-7577 CVE-2020-7578 CVE-2020-7584 CVE-2020-7593
- CVE-2019-18336 CVE-2020-7592 CVE-2020-10037 CVE-2020-10038 CVE-2020-10039 CVE-2020-10040 CVE-2020-10041 CVE-2020-10042 CVE-2020-10043
- CVE-2020-10044 CVE-2020-10045

Bilan de la vulnérabilité

Siemens a publié un correctif de sécurité concernant plusieurs produits SCADA. Une exploitation réussie de ces vulnérabilités pourrait permettre à un attaquant d'affecter la disponibilité, de lire des données sensibles et d'exécuter du code arbitraire à distance sur les appareils vulnérables.

Solution

Veuillez-vous référer au bulletin de sécurité Siemens du 15 Juillet 2020 afin d'installer les nouvelles mises à jour.

Risque

- Exécution du code arbitraire à distance;
- Déni de service ;
- Atteinte à la confidentialité ;

Référence

Bulletin de sécurité Siemens SSA-841348 du 14 juillet 2020:

- https://cert-portal.siemens.com/productcert/pdf/ssa-841348.pdf

Bulletin de sécurité Siemens SSA-631949 du 14 juillet 2020:

- https://cert-portal.siemens.com/productcert/pdf/ssa-631949.pdf

Bulletin de sécurité Siemens SSA-604937 du 14 juillet 2020:

- https://cert-portal.siemens.com/productcert/pdf/ssa-604937.pdf

Bulletin de sécurité Siemens SSA-589181 du 14 juillet 2020:

- https://cert-portal.siemens.com/productcert/pdf/ssa-589181.pdf

Bulletin de sécurité Siemens SSA-573753 du 14 juillet 2020:

- https://cert-portal.siemens.com/productcert/pdf/ssa-573753.pdf

Bulletin de sécurité Siemens SSA-508982 du 10 mars 2020, mis à jour le 14 juillet 2020:

- https://cert-portal.siemens.com/productcert/pdf/ssa-508982.pdf

Bulletin de sécurité Siemens SSA-364335 du 14 juillet 2020:

- https://cert-portal.siemens.com/productcert/pdf/ssa-364335.pdf

Bulletin de sécurité Siemens SSA-305120 du 14 juillet 2020:

- https://cert-portal.siemens.com/productcert/pdf/ssa-305120.pdf