BEZPEČNOSTNÉ VAROVANIE

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☐ **Vysoká**	☒ **Kritická**	**CVSS skóre: 9.8**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Siemens produkty viacero zraniteľností

Popis

Spoločnosť Siemens vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

09.06.2020

CVE

CVE-2018-15361, CVE-2019-8258, CVE-2019-8259, CVE-2019-8260, CVE-2019-8261, CVE-2019-8262, CVE-2019-8263, CVE-2019-8264, CVE-2019-8265, CVE-2019-8266, CVE-2019-8267, CVE-2019-8268, CVE-2019-8269, CVE-2019-8270, CVE-2019-8271, CVE-2019-8272, CVE-2019-8273, CVE-2019-8274, CVE-2019-8275, CVE-2019-8276, CVE-2019-8277, CVE-2019-8280, CVE-2020-7580, CVE-2020-7585, CVE-2020-7586, CVE-2020-7589

IOC

-

Zasiahnuté systémy

SINUMERIK Access MyMachine /P2P verzie staršie ako 4.8
SINUMERIK PCU base Win10 software /IPC verzie staršie ako 14.00
SINUMERIK PCU base Win7 software /IPC verzie staršie ako 12.01 HF4
Siemens LOGO!8 BM (incl. SIPLUS variants)
SIMATIC PCS 7
SIMATIC PDM
SIMATIC STEP 7 v5.X verzie staršie ako 5.6 SP2 HF3
SINAMICS STARTER (containing STEP 7 OEM version) verzie staršie ako 5.4 HF1
SIMATIC Automation Tool
SIMATIC NET PC software verzie staršie ako v16 Upd3
SIMATIC PCS 7
SIMATIC PCS neo
SIMATIC ProSave
SIMATIC S7-1500 Software Controller
SIMATIC STEP 7 verzie staršie ako v5.6 SP2 HF3
SIMATIC STEP 7 (TIA Portal) v13
SIMATIC STEP 7 (TIA Portal) v14
SIMATIC STEP 7 (TIA Portal) v15
SIMATIC STEP 7 (TIA Portal) v16
SIMATIC WinCC OA v3.16 verzie staršie ako P018
SIMATIC WinCC OA v3.17 verzie staršie ako P003

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava

Mail: sk-cert@nbu.gov.sk
Mobil: +421 903 993 706
Tel: +421 2 6869 2915

SK-CERT
Naša značka:
01439/2020/SK-CERT-144

SIMATIC WinCC Runtime Professional v13
SIMATIC WinCC Runtime Professional v14
SIMATIC WinCC Runtime Professional v15
SIMATIC WinCC Runtime Professional v16
SIMATIC WinCC v7.4 verzie staršie ako v7.4 SP1 Update 14
SIMATIC WinCC v7.5 verzie staršie ako v7.5 SP1 Update 3
SINAMICS Startdrive
SINEC NMS
SINEMA Server
SINUMERIK ONE virtual
SINUMERIK Operate

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnený prístup k citlivým údajom
Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://cert-portal.siemens.com/productcert/txt/ssa-817401.txt
https://cert-portal.siemens.com/productcert/txt/ssa-689942.txt
https://cert-portal.siemens.com/productcert/txt/ssa-927095.txt
https://cert-portal.siemens.com/productcert/txt/ssa-312271.txt
https://www.us-cert.gov/ics/advisories/icsa-20-161-06
https://www.us-cert.gov/ics/advisories/icsa-20-161-05
https://www.us-cert.gov/ics/advisories/icsa-20-161-04
https://www.us-cert.gov/ics/advisories/icsa-20-161-03
https://talosintelligence.com/vulnerability_reports/TALOS-2020-1025
https://talosintelligence.com/vulnerability_reports/TALOS-2020-1024