BEZPEČNOSTNÝ BULLETIN

Týždeň 15. 01. 2019 - 15. 01. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Emerson DeltaV Distributed Control System zraniteľnosť	Vysoká	**8.8**
02.	Cisco Email Security Appliance (ESA) zraniteľnosti	Vysoká	**8.6**
03.	Qt viacero zraniteľností	Vysoká	**7.8**
04.	Siemens S7-1500 CPU DoS zraniteľnosti	Vysoká	**7.5**
05.	Siemens SIMATIC S7-300 CPU DoS zraniteľnosť	Vysoká	**7.5**
06.	Siemens EN100 Ethernet Communication Module of SWT3000 DoS zraniteľnosti	Vysoká	**7.5**
07.	Linux systemd viacero zraniteľností	Vysoká	**7.5**
08.	Wireshark viacero zraniteľností	Vysoká	**7.5**
09.	SSH scp viacero zraniteľností	Vysoká	**7.5**
10.	Intel SGX zraniteľnosti	Vysoká	**7.5**
11.	Huawei PCManager zraniteľnosti	Vysoká	**7.3**
12.	Omron CX-Protocol zraniteľnosť	Stredná	**6.6**
13.	Adobe Connect a Digital Editions zraniteľnosti	Stredná	**6.5**
14.	MapSVG Lite zraniteľnosť	Stredná	**5.8**
15.	Siemens SICAM A8000 Series DoS zraniteľnosť	Stredná	**5.3**

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:
01380/2019/TS/OKB-015

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.8**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Emerson DeltaV Distributed Control System zraniteľnosť

Popis

Spoločnosť Emerson vydala bezpečnostnú aktualizáciu na svoj produkt DeltaV DCS, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému neautentifikovanému útočníkovi spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

10.01.2019

CVE

CVE-2018-19021

Zasiahnuté systémy

Emerson DeltaV DCS verzie staršie ako 11.3.1, 11.3.2, 12.3.1, 13.3.1, 14.3, R5.1, R6

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od Internetu.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-19-010-01

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.6
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Cisco Email Security Appliance (ESA) zraniteľnosti

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na svoj produkt Cisco Email Security Appliance, ktoré opravujú viacero bezpečnostných zraniteľností v AsyncOS.
Bezpečnostné zraniteľnosti spočívajú v nesprávnom spracovaní prichádzajúcich e-mailových správ a umožňujú vzdialenému neautentifikovanému útočníkovi prostredníctvom zasielania e-mailových správ podpísaných s S/MIME alebo obsahujúcich veľké množstvo špecifických URL adries spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

09.01.2019

CVE

CVE-2018-15453, CVE-2018-15460

Zasiahnuté systémy

Cisco Email Security Appliance (ESA)

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190109-esa-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190109-esa-url-dos

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.8**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Qt viacero zraniteľností

Popis

Spoločnosť Qt Group vydala bezpečnostnú aktualizáciu na svoj produkt Qt, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nesprávnom spracovaní BMP súborov komponentom QBmpHandler a umožňuje vzdialenému neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

04.12.2018

CVE

CVE-2018-15518, CVE-2018-19865, CVE-2018-19869, CVE-2018-19870, CVE-2018-19871, CVE-2018-19873

Zasiahnuté systémy

Qt 5.11.3

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=59411
https://tools.cisco.com/security/center/viewAlert.x?alertId=59412
https://tools.cisco.com/security/center/viewAlert.x?alertId=59414
https://tools.cisco.com/security/center/viewAlert.x?alertId=59415
https://tools.cisco.com/security/center/viewAlert.x?alertId=59416

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.5
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Siemens S7-1500 CPU DoS zraniteľnosti

Popis

Spoločnosť Siemens vydala bezpečnostnú aktualizáciu na svoj produkt S7-1500 CPU, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených paketov na porte 80/TCP a 443/TCP spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

08.01.2019

CVE

CVE-2018-16558, CVE-2018-16559

Zasiahnuté systémy

Siemens S7-1500 CPU verzie staršie ako 2.5

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od Internetu.

Zdroje

https://cert-portal.siemens.com/productcert/pdf/ssa-180635.pdf

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.5
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Siemens SIMATIC S7-300 CPU DoS zraniteľnosť

Popis

Spoločnosť Siemens vydala bezpečnostnú aktualizáciu na svoj produkt SIMATIC S7-300 CPU, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených paketov spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

08.01.2019

CVE

CVE-2018-16561

Zasiahnuté systémy

Siemens SIMATIC S7-300 CPU verzie staršie ako V3.X.16

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od Internetu.

Zdroje

https://cert-portal.siemens.com/productcert/pdf/ssa-306710.pdf

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.5
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Siemens EN100 Ethernet Communication Module of SWT3000 DoS zraniteľnosti

Popis

Spoločnosť Siemens vydala bezpečnostnú aktualizáciu na svoj produkt EN100 Ethernet Communication Module, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených paketov na porte 102/TCP spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

08.01.2019

CVE

CVE-2018-11451, CVE-2018-11452

Zasiahnuté systémy

Firmvér IEC 61850 EN100 Ethernet communication module pre SWT 3000 verzie staršie ako V4.33

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Odporúčame tiež firewallom zablokovať prístup na port 102/TCP. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od Internetu.

Zdroje

https://cert-portal.siemens.com/productcert/pdf/ssa-325546.pdf

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.5
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Linux systemd viacero zraniteľností

Popis

Bezpečnostní výskumníci informovali o bezpečnostných zraniteľnostiach v komponente linuxových operačných systémov systemd.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza vo funkcii journald a umožňuje vzdialenému autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

10.01.2019

CVE

CVE-2018-16864, CVE-2018-16865, CVE-2018-16866

Zasiahnuté systémy

OS Linux okrem SUSE Linux Enterprise 15, openSUSE Leap 15.0, Fedora 28 a 29

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://nvd.nist.gov/vuln/detail/CVE-2018-16864
https://nvd.nist.gov/vuln/detail/CVE-2018-16865
https://nvd.nist.gov/vuln/detail/CVE-2018-16866
https://www.qualys.com/2019/01/09/system-down/system-down.txt
https://www.bleepingcomputer.com/news/security/linux-systemd-affected-by-memory-corruption-vulnerabilities-no-patches-yet/
https://access.redhat.com/security/cve/cve-2018-16865

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.5
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Wireshark viacero zraniteľností

Popis

Vývojári analyzátora sieťovej prevádzky Wireshark vydali aktualizáciu svojho produktu, ktorá rieši viacero chýb a bezpečnostné zraniteľnosti spôsobené nedostatočným overovaním používateľských vstupov.
Bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených paketov spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

08.01.2019

CVE

CVE-2019-5716, CVE-2019-5717, CVE-2019-5718, CVE-2019-5719, CVE-2019-5721

Zasiahnuté systémy

Wireshark verzie staršie ako 2.6.6

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=59446
https://tools.cisco.com/security/center/viewAlert.x?alertId=59443
https://tools.cisco.com/security/center/viewAlert.x?alertId=59447
https://tools.cisco.com/security/center/viewAlert.x?alertId=59444
https://tools.cisco.com/security/center/viewAlert.x?alertId=59445

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.5
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

SSH scp viacero zraniteľností

Popis

Bezpečnostní výskumníci informovali o viacerých bezpečnostných zraniteľnostiach v scp klientovi v OpenSSH, WinSCP a PuTTY PSCP.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje útočníkovi, ktorý prevádzkuje škodlivý server získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

11.01.2019

CVE

CVE-2018-20684, CVE-2018-20685, CVE-2019-6109, CVE-2019-6110, CVE-2019-6111

Zasiahnuté systémy

OpenSSH 7.9
WinSCP verzie staršie ako 5.14
PuTTY PSCP

Následky

Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://seclists.org/oss-sec/2019/q1/63
https://exchange.xforce.ibmcloud.com/vulnerabilities/155484
https://sintonen.fi/advisories/scp-client-multiple-vulnerabilities.txt

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.5
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Intel SGX zraniteľnosti

Popis

Spoločnosť Intel vydala bezpečnostnú aktualizáciu na svoj produkt Intel SGX, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu autentifikovanému útočníkovi eskalovať
svoje privilégiá na napadnutom systéme.

Dátum prvého zverejnenia varovania

08.01.2019

CVE

CVE-2018-12155, CVE-2018-18098

Zasiahnuté systémy

Intel SGX SDK verzie staršie ako 2.2.100
Intel SGX Platform Software verzie staršie ako 2.2.100

Následky

Eskalácia privilégií
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.intel.com/content/www/us/en/security-center/advisory/INTEL-SA-00203.html
https://www.theregister.co.uk/2019/01/14/intel_patches_sgx_flaw/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.3**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Huawei PCManager zraniteľnosti

Popis

Spoločnosť Huawei vydala bezpečnostnú aktualizáciu na svoj produkt PCManager, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti umožňujú lokálnemu neautentifikovanému útočníkovi eskalovať svoje privilégiá na napadnutom systéme a vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

09.01.2019

CVE

CVE-2019-5241, CVE-2019-5242

Zasiahnuté systémy

Huawei PCManager verzie staršie ako 9.0.1.50

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20190109-01-pcmanager-en
https://exchange.xforce.ibmcloud.com/vulnerabilities/155329
https://exchange.xforce.ibmcloud.com/vulnerabilities/155328

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.6
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Omron CX-Protocol zraniteľnosť

Popis

Spoločnosť Omron vydala bezpečnostnú aktualizáciu na svoj produkt CX-Protocol, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje lokálnemu neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených projektových súborov vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

10.01.2019

CVE

CVE-2018-19027

Zasiahnuté systémy

CX-Protocol verzie staršie ako 2.01

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-19-010-02

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.5
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Adobe Connect a Digital Editions zraniteľnosti

Popis

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoje produkty Adobe Connect a Digital Editions, ktoré opravujú dve bezpečnostné zraniteľnosti.
Bližšie nešpecifikované bezpečnostné zraniteľnosti umožňujú útočníkovi získať neoprávnený prístup k citlivým údajom a eskalovať svoje privilégiá.

Dátum prvého zverejnenia varovania

08.01.2019

CVE

CVE-2018-12817, CVE-2018-19718

Zasiahnuté systémy

Adobe Connect verzie staršie ako 10.1
Adobe Adobe Digital Editions verzie staršie ako 4.5.10

Následky

Neoprávnený prístup k citlivým údajom
Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://helpx.adobe.com/security/products/connect/apsb19-05.html
https://helpx.adobe.com/security/products/Digital-Editions/apsb19-04.html

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 5.8
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

MapSVG Lite zraniteľnosť

Popis

Vývojári zásuvného modulu MapSVG Lite pre redakčný systém Wordpress vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v chýbajúcom overovaní hodnoty nonce počas modifikácie zverejňovaných dát a umožňuje vzdialenému útočníkovi vykonávať operácie s právami prihláseného používateľa.

Dátum prvého zverejnenia varovania

08.01.2019

CVE

-

Zasiahnuté systémy

MapSVG Lite 3.3.0

Následky

Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://seclists.org/fulldisclosure/2019/Jan/19

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 5.3
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Siemens SICAM A8000 Series DoS zraniteľnosť

Popis

Spoločnosť Siemens vydala bezpečnostné aktualizácie na svoje produkty SICAM A8000 RTU, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených paketov na porte 80/TCP a 443/TCP spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

08.01.2019

CVE

CVE-2018-13798

Zasiahnuté systémy

Siemens SICAM A8000 CP-8000 verzie staršie ako V14
Siemens SICAM A8000 CP-802X verzie staršie ako V14
Siemens SICAM A8000 CP-8050 verzie staršie ako V2.00

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od Internetu.

Zdroje

https://cert-portal.siemens.com/productcert/pdf/ssa-579309.pdf