BEZPEČNOSTNÝ BULLETIN

Týždeň 12. 12. 2018 – 18. 12. 2018

OBSAH BEZPEČNOSTNÉHO BULLETINU

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:
02049/2018/TS/OKB-210

BEZPEČNOSTNÝ BULLETIN

Týždeň 12. 12. 2018 – 18. 12. 2018

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

Identifikátor

Mozilla Firefox viacero zraniteľností

Popis

Spoločnosť Mozilla vydala bezpečnostné aktualizácie, ktoré opravujú viacero zraniteľností v internetových prehliadačoch Firefox a Firefox ESR. Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód na napadnutom systéme

Dátum prvého zverejnenia varovania

11.12.2018

CVE

CVE-2018-12405, CVE-2018-12406, CVE-2018-12407, CVE-2018-17466, CVE-2018-18492, CVE-2018-18493, CVE-2018-18494, CVE-2018-18495, CVE-2018-18496, CVE-2018-18497, CVE-2018-18498

Zasiahnuté systémy

Mozilla Firefox staršie ako 64
Mozilla Firefox ESR staršie ako 60.4

Následky

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

Odporúčania

Používateľom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://www.mozilla.org/en-US/security/advisories/mfsa2018-29/
https://www.mozilla.org/en-US/security/advisories/mfsa2018-30/

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

Identifikátor

phpMyAdmin zraniteľnosti

Popis

Vývojári phpMyAdmin vydali aktualizáciu svojho produktu, ktorá rieši viacero chýb a bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti umožňujú vzdialenému neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

11.12.2018

CVE

CVE-2018-19968, CVE-2018-19969, CVE-2018-19970

Zasiahnuté systémy

phpMyAdmin verzie staršie ako 4.8.4.

Následky

Neoprávnená zmena v systéme
Zneprístupnenie služby
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.phpmyadmin.net/news/2018/12/11/security-fix-phpmyadmin-484-released/
https://thehackernews.com/2018/12/phpmyadmin-security-update.html

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

Identifikátor

Google Chrome Stable Channel Update

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu, ktorá opravuje viacero chýb a bezpečnostnú zraniteľnosť v internetovom prehliadači Chrome.
Bezpečnostnú zraniteľnosť v komponente PDFium by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu v kontexte webového prehliadača a spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

12.12.2018

CVE

CVE-2018-17481

Zasiahnuté systémy

Google Chrome verzie staršie ako 71.0.3578.98

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://chromereleases.googleblog.com/search/label/Stable%20updates
https://www.cisecurity.org/advisory/a-vulnerability-in-google-chrome-could-allow-for-arbitrary-code-execution_2018-140/

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

Identifikátor

SQLite "Magellan" zraniteľnosť

Popis

Vývojári databázového systému SQLite vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť v komponente Chromium.
Bližšie nešpecifikovaná bezpečnostná umožňuje vzdialenému neautentifikovanému útočníkovi vykonať škodlivý kód a spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

01.12.2018

CVE

-

Zasiahnuté systémy

SQLite verzie staršie ako 3.26.0

Následky

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

Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie nepoužívajú databázový systém SQLite v zraniteľných verziách. V prípade, že áno, zabezpečte aktualizáciu systému.

Zdroje

https://www.sqlite.org/releaselog/3_26_0.html
https://blade.tencent.com/magellan/index_en.html
https://thehackernews.com/2018/12/sqlite-vulnerability.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.1**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Apache CouchDB zraniteľnosť

Popis

Vývojári databázového systému Apache CouchDB vydali aktualizáciu svojho produktu, ktorá rieši viacero chýb a bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému neautentifikovanému útočníkovi eskalovať svoje privilégiá na napadnutom systéme.

Dátum prvého zverejnenia varovania

17.12.2018

CVE

CVE-2018-17188

Zasiahnuté systémy

Apache CouchDB 2.3.0

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://seclists.org/oss-sec/2018/q4/255
https://exchange.xforce.ibmcloud.com/vulnerabilities/154346

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

Identifikátor

WordPress bezpečnostné zraniteľnosti

Popis

Vývojári redakčného systému WordPress vydali aktualizáciu svojho produktu, ktorá rieši sedem bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť umožňuje vzdialenému neautentifikovanému útočníkovi prostredníctvom špecifických vyhľadávacích reťazcov získať prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

13.12.2018

CVE

CVE-2018-20147, CVE-2018-20148, CVE-2018-20149, CVE-2018-20150, CVE-2018-20151, CVE-2018-20152, CVE-2018-20153

Zasiahnuté systémy

WordPress verzie staršie ako 5.0.1

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky nie sú založené na redakčnom systéme Wordpress v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu redakčného systému a pluginov.

Zdroje

https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/
https://www.bleepingcomputer.com/news/security/wordpress-security-patch-addresses-privacy-leak-bug/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.4**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

GE Mark VIe zraniteľnosť

Popis

Spoločnosť GE vydala bezpečnostné aktualizácie na svoje kontrolné systémy Mark VIe, EX2100e, EX2100e_Reg a LS2100e, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi, nachádzajúcemu sa v rovnakom sieťovom segmente získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

13.12.2018

CVE

CVE-2018-19003

Zasiahnuté systémy

Mark VIe verzie 03.03.28C až 05.02.04C,
EX2100e verzie staršie ako v04.09.00C,
EX2100e_Reg verzie staršie ako v04.09.00C
LS2100e verzie staršie ako v04.09.00C

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov a vypnúť webový server, pokiaľ nie je potrebný. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-18-347-04

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

Identifikátor

EcoStruxure Power Monitoring Expert zraniteľnosť

Popis

Spoločnosť EcoStruxure vydala bezpečnostné aktualizácie na svoje produkty Power Monitoring Expert, Energy Expert a Power SCADA Operation, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje vzdialenému neautentifikovanému útočníkovi prostredníctvom podvrhnutia upravených URL adries získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

13.12.2018

CVE

CVE-2018-7797

Zasiahnuté systémy

EcoStruxure™ Power Monitoring Expert (PME) v8.2, v9.0
EcoStruxure™ Energy Expert 1.3, v2.0
EcoStruxure™ Power SCADA Operation (PSO) 8.2, 9.0 Advanced Reports and Dashboards Module

Následky

Neoprávnená zmena v systéme
Neoprávnený prístup k citlivým údajom

Odporúčania

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

Zdroje

https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SEVD-2018-347-01+Power+Monitoring+Expert+and+Energy+Expert.pdf

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.2**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Geutebrück E2 Series IP kamery zraniteľnosť

Popis

Spoločnosť Geutebrück vydala bezpečnostnú aktualizáciu na svoje IP kamery radu E2, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému autentifikovanému útočníkovi vykonať škodlivé príkazy v zasiahnutom systéme.

Dátum prvého zverejnenia varovania

13.12.2018

CVE

CVE-2018-19007

Zasiahnuté systémy

Geutebrück E2 Series IP kamery firmvér verzie staršie ako 1.12.0.25

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-18-347-03