BEZPEČNOSTNÝ BULLETIN

Týždeň 09. 05. 2018 – 15. 05. 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-051

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

Identifikátor

Huawei iBMC Products Security Bypass

Popis

Spoločnosť Huawei vydala aktualizáciu na svoj produkt iBMC, ktorá opravuje bezpečnostnú zraniteľnosť spočívajúcu v nedostatočnej implementácii bezpečnostných mechanizmov. Uvedenú zraniteľnosť by vzdialený autentifikovaný útočník mohol prostredníctvom podvrhnutia špeciálne vytvorených správ zneužiť na upload autentifikačných certifikátov a následnú eskaláciu privilégií na zasiahnutých systémoch.

Dátum prvého zverejnenia varovania

09.05.2018

CVE

CVE-2018-7941

Zasiahnuté systémy

Huawei iBMC V200R002C60

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých produktov.

Zdroje

http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20180509-01-bypass-en
https://exchange.xforce.ibmcloud.com/vulnerabilities/143110

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

Identifikátor

Security Vulnerabilities Fixed in Firefox 60 and Firefox ESR 52.8

Popis

Spoločnosť Mozilla vydala bezpečnostné aktualizácie, ktoré riešia viacero zraniteľností v produktoch Firefox a Firefox ESR.
Najvážnejšie bezpečnostné zraniteľnosti by vzdialený neautentifikovaný útočník mohol prostredníctvom podvrhnutia špeciálne vytvoreného webového obsahu zneužiť na vykonanie škodlivého kódu a spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

09.08.2018

CVE

CVE-2018-5150, CVE-2018-5151, CVE-2018-5152, CVE-2018-5153, CVE-2018-5154, CVE-2018-5155, CVE-2018-5157, CVE-2018-5158, CVE-2018-5159, CVE-2018-5160, CVE-2018-5163, CVE-2018-5164, CVE-2018-5165, CVE-2018-5166, CVE-2018-5167, CVE-2018-5168, CVE-2018-5169, CVE-2018-5172, CVE-2018-5173, CVE-2018-5174, CVE-2018-5175, CVE-2018-5176, CVE-2018-5177, CVE-2018-5178, CVE-2018-5180, CVE-2018-5181, CVE-2018-5182, CVE-2018-5183

Zasiahnuté systémy

Firefox 60
Firefox ESR 52.8

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.mozilla.org/en-US/security/advisories/mfsa2018-12/
https://www.mozilla.org/en-US/security/advisories/mfsa2018-11/

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

Identifikátor

Adobe Products Security Vulnerabilities

Popis

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoje produkty Flash Player, Connect, Creative Cloud Desktop Application, Adobe Photoshop CC, Adobe Acrobat a Adobe Reader, ktoré opravujú viacero bezpečnostných zraniteľností.

Najzávažnejšia je bezpečnostná zraniteľnosť v Adobe Flash Player, ktorú by vzdialený neautentifikovaný útočník mohol prostredníctvom podvrhnutia škodlivého webového obsahu zneužiť na vykonanie škodlivého kódu a získanie úplnej kontroly nad systémom.

Zraniteľnosti v Adobe Acrobat a Adobe Reader by vzdialený neautentifikovaný útočník mohol prostredníctvom podvrhnutia špeciálne vytvorených súborov zneužiť na vykonanie škodlivého kódu v kontexte prihláseného používateľa.

Ostatné zraniteľnosti by útočník mohol zneužiť na neoprávnený prístup do systému a následnú eskaláciu privilégií.

Dátum prvého zverejnenia varovania

08.05.2018

CVE

CVE-2018-4873, CVE-2018-4944, CVE-2018-4946, CVE-2018-4947, CVE-2018-4948, CVE-2018-4949, CVE-2018-4950, CVE-2018-4951, CVE-2018-4952, CVE-2018-4953, CVE-2018-4954, CVE-2018-4955, CVE-2018-4956, CVE-2018-4957, CVE-2018-4958, CVE-2018-4959, CVE-2018-4960, CVE-2018-4961, CVE-2018-4962, CVE-2018-4963, CVE-2018-4964, CVE-2018-4965, CVE-2018-4966, CVE-2018-4967, CVE-2018-4968, CVE-2018-4969, CVE-2018-4970, CVE-2018-4971, CVE-2018-4972, CVE-2018-4973, CVE-2018-4974, CVE-2018-4975, CVE-2018-4976, CVE-2018-4977, CVE-2018-4978, CVE-2018-4979, CVE-2018-4980, CVE-2018-4981, CVE-2018-4982, CVE-2018-4983, CVE-2018-4984, CVE-2018-4985, CVE-2018-4986, CVE-2018-4987, CVE-2018-4988, CVE-2018-4989, CVE-2018-4990, CVE-2018-4991, CVE-2018-4992, CVE-2018-4993, CVE-2018-4994

Zasiahnuté systémy

Adobe Creative Cloud Desktop Application 4.4.1.298 a staršie
Adobe Flash Player verzia 29.0.0.140 a staršie
Adobe Connect 9.7.5 a staršie
Adobe Photoshop CC 2018 verzia 19.1.3 a staršie
Photoshop CC 2017 verzia 19.1.3 a staršie
Acrobat DC verzia 2018.011.20038 a staršie
Acrobat Reader DC verzia 2018.011.20038 a staršie
Acrobat 2017 verzia 2017.011.30079 a staršie
Acrobat Reader 2017 verzia 2017.011.30079 a staršie
Acrobat DC (classic 2015) verzia 2015.006.30417 a staršie
Acrobat Reader DC (classic 2015) verzia 2015.006.30417 a staršie

Následky
Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému; Eskalácia privilégií; Neoprávnený prístup do systému

Odporúčania
Administrátorom a používateľom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých produktov.

Zdroje
https://helpx.adobe.com/security/products/creative-cloud/apsb18-12.html https://helpx.adobe.com/security/products/flash-player/apsb18-16.html https://helpx.adobe.com/security/products/connect/apsb18-18.html https://helpx.adobe.com/security/products/acrobat/apsb18-09.html https://helpx.adobe.com/security/products/photoshop/apsb18-17.html

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

Identifikátor

Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu, ktorá rieši viacero zraniteľností v internetovom prehliadači Chrome.
Najvážnejšie bezpečnostné zraniteľnosti by vzdialený neautentifikovaný útočník mohol prostredníctvom podvrhnutia škodlivého webového obsahu zneužiť na vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

10.05.2018

CVE

CVE-2018-6120, CVE-2018-6121, CVE-2018-6122

Zasiahnuté systémy

Google Chrome verzie staršie ako 66.0.3359.170

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://chromereleases.googleblog.com/2018/05/stable-channel-update-for-desktop.html
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-chrome-could-allow-for-arbitrary-code-execution_2018-055/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.4**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Lenovo Systems Vulnerabilities

Popis

Spoločnosť Lenovo vydala bezpečnostné aktualizácie na svoje produkty System x server a notebooky ThinkPad, ktoré opravujú viacero bezpečnostných zraniteľností v administrátorskej konzole.
Bezpečnostná zraniteľnosť v komponente Lenovo System Update Drive Mapping Utility (C:\Program Files\Lenovo\System Update\mapdrv.exe) spočíva v nedostatočnom overovaní používateľských vstupov počas autentifikácie a lokálny útočník by ju mohol prostredníctvom podvrhnutia špeciálnych vstupov zneužiť na vyvolanie pretečenia zásobníka a následné vykonanie škodlivého kódu v kontexte prihláseného používateľa.
Bezpečnostná zraniteľnosť v Lenovo System x Secure Boot spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a útočník s fyzickým prístupom k systému by ju mohol zneužiť na vykonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

03.05.2018

CVE

CVE-2017-3775, CVE-2018-9063

Zasiahnuté systémy

notebooky ThinkPad obsahujúce Lenovo System Update verzie staršie ako 5.07.0072
Flex System x
NeXtScale nx360 M5

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://support.lenovo.com/sk/en/solutions/len-20241
https://support.lenovo.com/sk/en/solutions/len-19625
https://exchange.xforce.ibmcloud.com/vulnerabilities/142705
https://exchange.xforce.ibmcloud.com/vulnerabilities/142706
https://threatpost.com/lenovo-patches-arbitrary-code-execution-flaw/131725/

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

Identifikátor

PowerDNS Authoritative Dnsreplay Tool Buffer Overflow Vulnerability

Popis

Spoločnosť PowerDNS vydala aktualizáciu, ktorá rieši bezpečnostnú zraniteľnosť v produkte PowerDNS Authoritative Server.
Bezpečnostnú zraniteľnosť nachádzajúcu sa v nástroji dnsreplay by vzdialený neautentifikovaný útočník mohol prostredníctvom podvrhnutia špeciálneho PCAP súboru zneužiť na vyvolanie pretečenia zásobníka a následné vykonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

08.05.2018

CVE

CVE-2018-1046

Zasiahnuté systémy

PowerDNS Authoritative verzie 4.0.0 až 4.1.1

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých produktov. Rovnako odporúčame nepoužívať nástroj dnsreplay na spracovanie PCAP súborov pochádzajúcich z neoverených zdrojov.

Zdroje

https://doc.powerdns.com/authoritative/security-advisories/powerdns-advisory-2018-02.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/143070
http://seclists.org/oss-sec/2018/q2/97

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

Identifikátor

Silex Technology SX-500/SD-320AN or GE Healthcare MobileLink

Popis

Spoločnosť Silex Technology vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú viacero bezpečnostných zraniteľností.
Najvážnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a vzdialený autentifikovaný útočník by ju mohol prostredníctvom podvrhnutia špeciálnych POST požiadaviek zneužiť na vykonanie škodlivého kódu a neoprávnenú úpravu nastavení systému.

Dátum prvého zverejnenia varovania

08.05.2018

CVE

CVE-2018-6020, CVE-2018-6021

Zasiahnuté systémy

GEH-500 Version 1.54 a staršie (integrovaný do GE MobileLink), SX-500 všetky verzie
GEH-SD-320AN verzie GEH-1.1 a staršie (integrovaný do GE MobileLink)
SD-320AN verzie 2.01 a staršie
GE MAC Resting ECG MAC 3500
GE MAC Resting ECG MAC 5000
GE MAC Resting ECG MAC 5500
GE MAC Resting ECG MAC 5500 HD

Následky

Vykonanie škodlivého kódu, Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov, aplikovať firewallové pravidlá a limitovať prístup k zasiahnutým zariadeniam a ich funkciám zavedením zoznamu pre riadenie prístupov ACL. Taktiež odporúčame vo webovom rozhraní povoliť "update" konto a zadať preň nové heslo, čím sa zabráni neoprávneným zmenám v nastaveniach systému.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSMA-18-128-01
https://exchange.xforce.ibmcloud.com/vulnerabilities/143020
https://exchange.xforce.ibmcloud.com/vulnerabilities/143021

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

Identifikátor

Node.js Electron Module Code Execution

Popis

Vývojári webového frameworku Electron vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť v Node.js komponente.
Bezpečnostná zraniteľnosť spočíva v nesprávnom spracovávaní hodnôt vo Webviews a umožňuje vzdialený útočník by ju mohol zneužiť na vykonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

25.03.2018 (posledná aktualizácia 10.05.2018)

CVE

CVE-2018-1000136

Zasiahnuté systémy

Electron verzie staršie ako 1.8.4

Následky

Vykonanie škodlivého kódu

Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie nie sú založené na frameworku Electron v zraniteľných verziách. V prípade, že áno, zabezpečte aktualizáciu frameworku.

Zdroje

https://www.trustwave.com/Resources/SpiderLabs-Blog/CVE-2018-1000136---Electron-nodeIntegration-Bypass/
https://exchange.xforce.ibmcloud.com/vulnerabilities/140838

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

Identifikátor

OpenPGP and S/MIME Mail Client eFail Vulnerabilities

Popis

Výskumníci upozorňujú na bezpečnostné zraniteľnosti emailových klientov podporujúcich štandardy PGP a S/MIME určené pre šifrovaný prenos e-mailov. Bezpečnostné zraniteľnosti spočívajú v nesprávnej implementácii mechanizmov spracovania HTML e-mailov a načítavania obsahu z externých zdrojov a vzdialený útočník by ich prostredníctvom podvrhnutia špeciálne upravených šifrovaných e-mailov mohol zneužiť na získanie prístupu k citlivým údajom v ich dešifrovanej podobe, vrátane údajov v minulých e-mailoch.

Dátum prvého zverejnenia varovania

14.05.2018

CVE

CVE-2017-17688, CVE-2017-17689

Zasiahnuté systémy

9Folders, Inc.; Airmail; Apple Mail; iOS Mail; eM Client; Evolution; Flipdog Solutions, LLC; GnuPG; Google Gmail; GPGTools; IBM Corporation; KMail; MailMate; Microsoft Outlook; Microsoft Win 10 mail; Mozilla Thunderbird; Postbox; R2Mail2; Ritlabs, SRL; Roundcube; The Enigmail Project; The Horde Project; Trojita

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Na uvedené zraniteľnosti v súčasnosti nie sú dostupné aktualizácie. Na znemožnenie zneužitia týchto zraniteľností Vám odporúčame:

- na dešifrovanie prichádzajúcich e-mailových správ použite externé aplikácie,
- v nastaveniach e-mailových klientov vypnite funkciu renderovania HTML obsahu,
- v nastaveniach e-mailových klientov vypnite automatické sťahovanie obsahu zo vzdialených zdrojov (obrázky).

Tiež odporúčame sledovať stránky výrobcov zasiahnutých e-mailových klientov a po vydaní bezpečnostných záplat bezodkladne vykonať aktualizáciu.

Zdroje

https://www.kb.cert.org/vuls/id/122919
https://efail.de/
https://thehackernews.com/2018/05/efail-pgp-email-encryption.html

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

Identifikátor

SAP Security Patch Day – May 2018

Popis

Spoločnosť SAP vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť v produkte SAP Internet Graphics Server (IGS) je spôsobená nedostatočným overovaním používateľských vstupov a vzdialený útočník by ju mohol prostredníctvom podvrhnutia špeciálne vytvorenej HTTP požiadavky zneužiť na vykonanie škodlivého kódu alebo zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

08.05.2018

CVE

CVE-2018-2415, CVE-2018-2416, CVE-2018-2417, CVE-2018-2418, CVE-2018-2419, CVE-2018-2420, CVE-2018-2421, CVE-2018-2422, CVE-2018-2423

Zasiahnuté systémy

SAP Internet Graphics Server
SAP MaxDB ODBC driver
SAP Identity Management
SAP NetWeaver Application Server
SAP Enterprise Financial Services

Následky

Vykonanie škodlivého kódu, Zneprístupnenie služby, Neoprávnený prístup k citlivým údajom, Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://blogs.sap.com/2018/05/08/sap-security-patch-day-may-2018/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 6.4**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Micro Focus HP Service Manager SQL Injection Vulnerability

Popis

Spoločnosť Micro Focus vydala bezpečnostnú aktualizáciu na svoj produkt HP Service Manager, ktorá opravuje bezpečnostnú zraniteľnosť v komponente Service Manager Web Tier.

Uvedená zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a vzdialený autentifikovaný útočník by mohol zneužiť na vykonanie SQL injekcie a následne zobraziť, pridať, upraviť alebo odstrániť údaje uložené v backend databáze.

Dátum prvého zverejnenia varovania

10.05.2018

CVE

CVE-2018-6494

Zasiahnuté systémy

Micro Focus HP Service Manager Software verzie 9.30 až 9.35, 9.40, 9.41, 9.50, 9.51

Následky

Neoprávnený prístup k citlivým údajom, Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu dotknutého softvéru. Po vykonaní aktualizácie odporúčame preveriť integritu databázy a prístupové logy na prítomnosť pokusov o SQL injekciu.

Zdroje

https://softwaresupport.softwaregrp.com/document/-/facetsearch/document/KM03158656
https://exchange.xforce.ibmcloud.com/vulnerabilities/143189
https://securitytracker.com/id?1040902

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-051