BEZPEČNOSTNÝ BULLETIN

Týždeň 04. 07. 2018 – 10. 07. 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-086

BEZPEČNOSTNÝ BULLETIN

Týždeň 04. 07. 2018 – 10. 07. 2018

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

Identifikátor

Apple Releases Security Updates July 2018

Popis

Spoločnosť Apple vydala bezpečnostné aktualizácie na svoje produkty macOS, iOS, watchOS, tvOS, iCloud for Windows, iTunes for Windows a Safari, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie zraniteľnosti v operačných systémoch OS X, macOS, iOS a tvOS sa nachádzajú v komponentoch APFS, ATS a Webkit a vzdialený neautentifikovaný útočník by ich mohol zneužiť na vykonanie škodlivého kódu s následkom úplného narušenie dôvernosti, integrity a dostupnosti systému.
Ostatné zraniteľnosti by vzdialený neautentifikovaný útočník mohol zneužiť na eskaláciu privilégií, zneprístupnenie služby alebo neoprávnený prístup k citlivým údajom.
Bezpečnostné aktualizácie pre OS X opravujú aj najnovšie verzie zraniteľností Lazy FP patriacich do rodiny procesorových zraniteľností Spectre.

Dátum prvého zverejnenia varovania

10.07.2018

CVE

CVE-2018-3665, CVE-2018-4178, CVE-2018-4248, CVE-2018-4260, CVE-2018-4261, CVE-2018-4262, CVE-2018-4263, CVE-2018-4264, CVE-2018-4265, CVE-2018-4266, CVE-2018-4267, CVE-2018-4268, CVE-2018-4269, CVE-2018-4270, CVE-2018-4271, CVE-2018-4272, CVE-2018-4273, CVE-2018-4274, CVE-2018-4275, CVE-2018-4277, CVE-2018-4278, CVE-2018-4280, CVE-2018-4282, CVE-2018-4283, CVE-2018-4284, CVE-2018-4285, CVE-2018-4289, CVE-2018-4290, CVE-2018-4293

Zasiahnuté systémy

OS X El Capitan 10.11.6
macOS Sierra 10.12.6
macOS High Sierra 10.13.5
watchOS verzie staršie ako 4.3.2
tvOS verzie staršie ako 11.4.1
iTunes for Windows verzie staršie ako 12.8, iCloud for Windows verzie staršie ako 7.6
Safari verzie staršie ako 11.1.2

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje
https://support.apple.com/en-us/HT208932
https://support.apple.com/en-us/HT208933
https://support.apple.com/en-us/HT208934
https://support.apple.com/en-us/HT208935
https://support.apple.com/en-us/HT208936
https://support.apple.com/en-us/HT208937
https://support.apple.com/en-us/HT208938

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

Identifikátor

Multiple Vulnerabilities in Mozilla Thunderbird Could Allow for Arbitrary Code Execution

Popis

Spoločnosť Mozilla vydala bezpečnostnú aktualizáciu na svoj produkt Mozilla Thunderbird, ktorá opravuje viacero bezpečnostných zraniteľností.
Najvážnejšie zraniteľnosti umožňujú vzdialenému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov spôsobiť vykonanie škodlivého kódu v kontexte privilegovaného procesu s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

05.07.2018

CVE

CVE-2018-12359, CVE-2018-12360, CVE-2018-12362, CVE-2018-12363, CVE-2018-12364, CVE-2018-12365, CVE-2018-12366, CVE-2018-12368, CVE-2018-12372, CVE-2018-12373, CVE-2018-12374, CVE-2018-5188

Zasiahnuté systémy

Mozilla Thunderbird verzie staršie ako 52.9

Následky

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

Odporúčania

Používateľom a administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy a prílohy z neznámych zdrojov.

Zdroje

https://www.mozilla.org/en-US/security/advisories/mfsa2018-18/
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-mozilla-thunderbird-could-allow-for-arbitrary-code-execution_2018-074/

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

Identifikátor

Arbitrary File Deletion Flaw Present in WordPress

Popis

Vývojári redakčného systému WordPress vydali aktualizáciu svojho produktu, ktorá rieši bezpečnostné zraniteľnosti spočívajúce v nedostatočnom overovaní používateľských vstupov a nedostatočnej implementácii bezpečnostných mechanizmov.
Uvedené zraniteľnosti by vzdialený autentifikovaný útočník mohol prostredníctvom podvrhnutia špeciálne vytvorených metadát počas nahrávania súborov zneužiť na odstránenie ľubovoľných súborov Wordpress inštalácie, získanie úplnej kontroly nad webovou stránkou a vykonanie škodlivého kódu s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

27.06.2018 (posledná aktualizácia 05.07.2018)

CVE

-

Zasiahnuté systémy

Wordpress verzie staršie ako 4.9.7

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
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 na najnovšiu verziu.

Zdroje

https://wordpress.org/news/2018/07/wordpress-4-9-7-security-and-maintenance-release/
https://www.wordfence.com/blog/2018/07/details-of-an-additional-file-deletion-vulnerability-patched-in-wordpress-4-9-7/
https://blog.ripstech.com/2018/wordpress-file-delete-to-code-execution/

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

Identifikátor

Multiple ADB Broadband Gateways / Routers Vulnerabilities

Popis

Spoločnosť Advanced Digital Broadcast (ADB) vydala bezpečnostné aktualizácie na svoje sieťové zariadenia založené na platforme Epicentro, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú vzdialenému autentifikovanému útočníkovi eskalovať svoje privilégiá na napadnutom systéme a vykonávať neoprávnené zmeny v napadnutom systéme.

Dátum prvého zverejnenia varovania

04.07.2018

CVE

CVE-2018-13108, CVE-2018-13109, CVE-2018-13110

Zasiahnuté systémy

Všetky zariadenia ADB Broadband Gateways / Routers založené na platforme Epicentro

Následky

Eskalácia privilégií, Neoprávnený prístup k citlivým údajom, Neoprávnený prístup do systému, Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

http://seclists.org/fulldisclosure/2018/Jul/17
http://seclists.org/fulldisclosure/2018/Jul/18
http://seclists.org/fulldisclosure/2018/Jul/19
https://threatpost.com/year-old-critical-vulnerabilities-patched-in-isp-broadband-gear/133702/

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

Identifikátor

RSA Products Multiple Vulnerabilities

Popis

Spoločnosť RSA vydala bezpečnostnú aktualizáciu na svoj produkt RSA Certificate Manager, ktorá opravuje bezpečnostnú zraniteľnosť v komponentoch RSA CMP Enroll Server a RSA REST Enroll Server.
Vzdialený neautentifikovaný útočník by túto zraniteľnosť mohol prostredníctvom podvrhnutia špeciálne vytvorených požiadaviek zneužiť na neoprávnený prístup k súborom uloženým na súborovom systéme zasiahnutého servera.
Spoločnosť tiež vydala odporúčania na riešenie bezpečnostnej zraniteľnosti nachádzajúcej sa v produktoch RSA Identity Governance and Lifecycle, RSA Via Lifecycle and Governance a RSA Identity Management & Governance.
Uvedená zraniteľnosť spočíva v nesprávnej konfigurácii produktu inštalačným skriptom a lokálny autentifikovaný útočník by ju mohol zneužiť na eskaláciu privilégií a vykonanie škodlivého kódu s administrátorskými právami.

Dátum prvého zverejnenia varovania

28.06.2018 (posledná aktualizácia 05.07.2018)

CVE

CVE-2018-11051, CVE-2018-11049

Zasiahnuté systémy

RSA Certificate Manager verzie 6.9 build 560 až build 564
RSA Identity Governance and Lifecycle verzi 7.1.0, 7.0.1, 7.0.2
RSA Via Lifecycle and Governance verzie 7.0 (Hardware Appliance, Software Bundle)
RSA Identity Management & Governance (RSA IMG) verzie 6.9.0, 6.9.1

Následky

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

Odporúčania

Administrátorom produktu RSA Certificate Manager odporúčame vykonať aktualizáciu zasiahnutých systémov. Administrátorom ostatných produktov odporúčame postupovať podľa odporúčaní spoločnosti RSA, ktoré sú pre ich klientov dostupné na stránke https://community.rsa.com/docs/DOC-94098

Zdroje
http://seclists.org/fulldisclosure/2018/Jul/11
https://www.securitytracker.com/id/1041211
http://seclists.org/fulldisclosure/2018/Jul/23
https://exchange.xforce.ibmcloud.com/vulnerabilities/145954

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

Identifikátor

Multiple Vulnerabilities in Apache Solr, CXF and PDFBox

Popis

Spoločnosť Apache vydala bezpečnostné aktualizácie, ktoré opravujú viacero bezpečnostných zraniteľností v produktoch Solr, CXF a PDFBox.
Zraniteľnosť v Apache Solr je spôsobená nedostatočným overovaním používateľských vstupov a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvoreného XML súboru mohol zneužiť na realizáciu XXE (XML External Entity) útoku a získať neoprávnený prístup k súborom uloženým na Solr serveri.
Najzávažnejšia zraniteľnosť v Apache CXF sa nachádza v plugine Fediz a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvorených XML DTD (Document Type Declarations) údajov mohol zneužiť na zneprístupnenie služby.
Zraniteľnosť v Apache PDFBox sa nachádza v komponente AFMParser a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvoreného PDF súboru mohol zneužiť na zneprístupnenie služby.

Dátum prvého zverejnenia varovania

04.07.2018

CVE

CVE-2018-8026, CVE-2018-8036, CVE-2018-8038, CVE-2018-8039

Zasiahnuté systémy

Apache Solr verzie 6.6.4, 7.3.1
Apache CXF Fediz verzie staršie ako 1.4.4.
Apache PDFBox verzie staršie ako 1.8.15 a 2.0.11

Následky

Zneprístupnenie služby, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/145827
https://issues.apache.org/jira/browse/SOLR-12450
https://exchange.xforce.ibmcloud.com/vulnerabilities/145828
http://cxf.apache.org/security-advisories.data/CVE-2018-8038.txt.asc
http://cxf.apache.org/security-advisories.data/CVE-2018-8039.txt.asc
https://tools.cisco.com/security/center/viewAlert.x?alertId=58380

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

Identifikátor

ISC BIND Denial of Service Vulnerability

Popis

Vývojári DNS servera BIND vydali aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť spôsobenú chybou pri prenose veľkých zónových súborov.
Uvedenú zraniteľnosť by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia veľkých zónových súborov mohol zneužiť na zneprístupnenie služby.
Zraniteľnosť sa týka autoritatívnych serverov, ktoré prijímajú zónové údaje prostredníctvom IXFR (Incremental Zone Transfer) alebo AXFR DNS dopytov z hlavného zdroja a ktoré nemajú príznak *ixfr-from-differences* nastavený na hodnotu *"no"*.

Dátum prvého zverejnenia varovania

03.07.2018 (posledná aktualizácia 05.07.2018)

CVE

-

Zasiahnuté systémy

BIND verzie 9.0.x až 9.8.8, 9.9.0 až 9.9.12, 9.10.0 až 9.10.7, 9.11.0 až 9.11.3, 9.12.0 až 9.12.1, vývojová vetva verzie 9.13.0 až 9.13.1

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Ak je to možné, odporúčame limitovať prenosy zónových súborov na dôveryhodné serveri zavedením zoznamu pre riadenie prístupov (ACL) na báze IP adries alebo prostredníctvom TSIG kľúčov.
Administrátorom serverov, ktoré musia prijímať zónové údaje z nedôveryhodných zdrojov odporúčame obmedziť veľkosť zónových súborov prostredníctvom *max-records* a nastavením príznaku *"ixfr-from-differences no;"*.

Zdroje

https://kb.isc.org/article/AA-01627
https://exchange.xforce.ibmcloud.com/vulnerabilities/145829

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 5.4**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Open-Xchange App Suite Multiple Vulnerabilities

Popis

Spoločnosť Open-Xchange vydala bezpečnostné aktualizácie, ktoré opravujú viacero bezpečnostných zraniteľností v produkte Open-Xchange App Suite.
Prvá zraniteľnosť spočíva v nedostatočnom filtrovaní HTML kódu v používateľských vstupoch a vzdialený neautentifikovaný útočník by ju mohol zneužiť na realizáciu XSS (Cross-Site Scripting) útoku, vykonanie škodlivého kódu v prehliadači a získanie prístupu k údajom uloženým v cookies, vrátane autentifikačných údajov.
Druhú zraniteľnosť by vzdialený autentifikovaný útočník prostredníctvom podvrhnutia špeciálne upraveného XML súboru mohol zneužiť na realizáciu XXE (XML External Entity) útoku a získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

03.06.2018

CVE

CVE-2018-9997, CVE-2018-9998

Zasiahnuté systémy

Open-Xchange App Suite

Následky

Vykonanie škodlivého kódu, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.securitytracker.com/id/1041213
http://seclists.org/fulldisclosure/2018/Jul/12

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

Identifikátor

"Stylish" Browser Extension Steals All Your Internet History

Popis

Spoločnosti Google a Mozilla odstránili zo svojich oficiálnych obchodov rozšírenie pre internetové prehliadače Stylish na základe zistení, podľa ktorých uvedené rozšírenie odosiela na vzdialené servery informácie o všetkých navštívených webových stránkach spolu s jedinečným identifikátorom používateľa.

Dátum prvého zverejnenia varovania

02.07.2018

CVE

-

Zasiahnuté systémy

Rozšírenie Stylish pre prehliadače Firefox, Chrome a Opera

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Používateľom a administrátorom odporúčame odinštalovať rozšírenie Stylish zo svojich internetových prehliadačov.

Zdroje

https://robertheaton.com/2018/07/02/stylish-browser-extension-steals-your-internet-history/
https://www.bleepingcomputer.com/news/software/chrome-and-firefox-pull-stylish-add-on-after-report-it-logged-browser-history/