BEZPEČNOSTNÝ BULLETIN

Týždeň 25. 04. 2018 – 01. 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-042

BEZPEČNOSTNÝ BULLETIN

Týždeň 25. 04. 2018 – 01. 05. 2018

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

Identifikátor

Hyland Perspective Document Filters Code Execution

Popis

Spoločnosť Hyland vydala bezpečnostnú aktualizáciu na svoj produkt Hyland Perspective Document Filters, ktorá opravuje viaceré bezpečnostné zraniteľnosti.
Najvážnejšia bezpečnostná zraniteľnosť umožňuje vzdialenému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov spôsobiť pretečenie zásobníka a vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

26.04.2018

CVE

CVE-2018-3855, CVE-2018-3851, CVE-2018-3845, CVE-2018-3844

Zasiahnuté systémy

Hyland Perceptive Document Filters 11.4.0.2547
Hyland Perceptive Document Filters 11.2.0.1732

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://www.talosintelligence.com/vulnerability_reports/TALOS-2018-0538
https://www.talosintelligence.com/vulnerability_reports/TALOS-2018-0534
https://www.talosintelligence.com/vulnerability_reports/TALOS-2018-0528
https://www.talosintelligence.com/vulnerability_reports/TALOS-2018-0527

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

Identifikátor

Chrome Stable Channel Update for Desktop

Popis

Spoločnosť Google vydala aktualizáciu svojho produkt Google Chrome, verzia 66.0.3359.139, ktorá obsahuje opravy viacerých chýb a 3 bezpečnostných zraniteľností. Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v komponente Media Cache a umožňuje vzdialenému útočníkovi prostredníctvom podvrhnutia škodlivého webového obsahu vykonať škodlivý kód v kontexte prihláseného používateľa.

Dátum prvého zverejnenia varovania

26.04.2018

CVE

CVE-2018-6118

Zasiahnuté systémy

Google Chrome verzie staršie ako 66.0.3359.139

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://chromereleases.googleblog.com/2018/04/stable-channel-update-for-desktop_26.html

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

Identifikátor

Multiple Vulnerabilities in PHP Could Allow for Arbitrary Code Execution

Popis

Vývojári skriptovacieho jazyka PHP vydali bezpečnostnú aktualizáciu, ktorá rieši viacero chýb a bezpečnostných zraniteľností.
Bližšie nešpecifikované zraniteľnosti by vzdialený útočník mohol zneužiť na vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

27.04.2018

CVE

-

Zasiahnuté systémy

PHP 7.2 verzie staršie ako 7.2.5
PHP 7.1 verzie staršie ako 7.1.17
PHP 7.0 verzie staršie ako 7.0.30
PHP 5.0 verzie staršie ako 5.6.36

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-php-could-allow-for-arbitrary-code-execution_2018-046/

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

Identifikátor

TP-Link Routers Vulnerable to Remote Code Execution

Popis

Výskumníci spoločnosti Fidus objavili bezpečnostnú zraniteľnosť v routroch TP-Link WR740N. Bezpečnostná zraniteľnosť umožňuje vzdialenému autentifikovanému útočníkovi, ktorý disponuje prihlasovacími údajmi eskalovať svoje privilégiá a vykonať škodlivý kód. Spoločnosť TP-Link doposiaľ nevydala aktualizácie riešiace uvedenú zraniteľnosť.
Obdobná bezpečnostná zraniteľnosť už bola v minulosti reportovaná pod označením CVE-2017-13772 v novšej rade routrov TL-WR940N, pre ktorú už bola vydaná bezpečnostná aktualizácia.

Dátum prvého zverejnenia varovania

26.04.2018

CVE

-

Zasiahnuté systémy

TP-Link WR740N

Následky

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

Odporúčania

Administrátorom odporúčame zmeniť predvolené prihlasovacie údaje do routra a použiť silné a komplexné heslo. Tiež odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.

Zdroje

https://www.fidusinfosec.com/a-curious-case-of-code-reuse-tplink-cve-2017-13772-v2/
http://seclists.org/fulldisclosure/2018/Apr/55
https://nvd.nist.gov/vuln/detail/CVE-2017-13772

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

Identifikátor

Apple Releases Security Updates

Popis

Spoločnosť Apple vydala bezpečnostné aktualizácie na svoje produkty macOS High Sierra, iOS a Safari, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie zraniteľnosti v produkte Safari by vzdialený neautentifikovaný útočník mohol prostredníctvom podvrhnutia špecifického webového obsahu zneužiť na vykonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

24.04.2018

CVE

CVE-2018-4200, CVE-2018-4204, CVE-2018-4206, CVE-2018-4187

Zasiahnuté systémy

Safari 11.1
macOS High Sierra 10.13.4
iOS 11.3.1

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://support.apple.com/en-us/HT208741
https://support.apple.com/en-us/HT208742
https://support.apple.com/en-us/HT208743

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

Identifikátor

Apache UIMA XML External Entity Expansion (XXE) Attack Exposure

Popis

Spoločnosť Apache vydala bezpečnostnú aktualizáciu na svoj produkt Apache UIMA, ktorá opravuje bezpečnostnú zraniteľnosť v XML parseri.
Bezpečnostná zraniteľnosť umožňuje vzdialenému autentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upraveného XML súboru vykonať XXE (XML External Entity) útok a získať citlivé údaje.

Dátum prvého zverejnenia varovania

26.04.2018

CVE

CVE-2017-15691

Zasiahnuté systémy

uimaj 2.x.x verzie staršie ako 2.10.2
uimaj 3.0.0 verzie staršie ako 3.0.0-beta
uima-as verzie staršie ako 2.10.2
uimaFIT verzie staršie ako 2.4.0
uimaDUCC verzie staršie ako 2.2.2

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/142433
http://seclists.org/oss-sec/2018/q2/76

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

Identifikátor

Eclipse Mosquitto Denial of Service Vulnerability

Popis

Produkt Eclipse Mosquitto obsahuje bezpečnostnú zraniteľnosť, ktorú by vzdialený neautentifikovaný útočník mohol prostredníctvom vytvorenia veľkého množstva spojení zneužiť na zaplnenie operačnej pamäte RAM a následné zneprístupnenie služby.

Dátum prvého zverejnenia varovania

24.04.2018 (posledná aktualizácia 25.04.2018)

CVE

CVE-2017-7651, CVE-2017-7652

Zasiahnuté systémy

Eclipse Mosquitto 1.4.14

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/142340

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.1**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Xen Hypervisor Multiple Vulnerabilities

Popis

Produkt Xen Hypervisor obsahuje viacero zraniteľností. Prvá zraniteľnosť spočíva v nesprávnom spracovávaní chybových stavov a lokálny útočník by prostredníctvom tejto zraniteľnosti mohol vyvolať pád hypervisora a spôsobiť tak zneprístupnenie služieb.
Druhá zraniteľnosť spočíva v nesprávnom spracovávaní súborov rôznych formátov na virtuálnych diskoch a vzdialený neautentifikovaný útočník by ju mohol prostredníctvom podvrhnutia špeciálneho CDROM obrazu zneužiť na získanie prístupu k citlivým údajom.
Túto zraniteľnosť je možné zneužiť len na x86 HVM systémoch.

Dátum prvého zverejnenia varovania

25.04.2018 (posledná aktualizácia 30.04.2018)

CVE

CVE-2018-10471

Zasiahnuté systémy

Xen

Následky

Zneprístupnenie služby, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

http://xenbits.xen.org/xsa/advisory-258.html
http://xenbits.xen.org/xsa/advisory-259.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/142368
https://exchange.xforce.ibmcloud.com/vulnerabilities/142369

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.1**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Delta Electronics PMSoft Vulnerabilities

Popis

Spoločnosť Delta Electronics vydala bezpečnostnú aktualizáciu na svoj produkt PMSoft. Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje lokálnemu útočníkovi prostredníctvom podvrhnutia špeciálne upravených .ppm súborov spôsobiť pretečenie zásobníka a následné vykonanie škodlivého kódu alebo zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

26.04.2018

CVE

CVE-2018-8839

Zasiahnuté systémy

PMSoft verzie staršie ako 2.11

Následky

Vykonanie škodlivého kódu, Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-18-116-01

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 6.3**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Advantech WebAccess HMI Designer Multiple Vulnerabilities

Popis

Spoločnosť Advantech vydala bezpečnostnú aktualizáciu na svoj produkt WebAccess HMI Designer, ktorá opravuje viacero bezpečnostných zraniteľností.
Uvedené zraniteľnosti by vzdialený neautentifikovaný útočník mohol prostredníctvom podvrhnutia špecifických .pm3 súborov zneužiť na vykonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

24.04.2018

CVE

CVE-2018-8833, CVE-2018-8835, CVE-2018-8837

Zasiahnuté systémy

Advantech WebAccess HMI Designer verzia 2.1.7.32 a staršie

Následky

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

Odporúčania

Na uvedené zraniteľnosti v súčasnosti nie sú dostupné aktualizácie. Administrátorom odporúčame aplikovať firewallové pravidlá a limitovať prístup k zasiahnutým systémom. Rovnako odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-18-114-03

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 6.2**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

ClamAV Clamscan PDF File Handling Remote Denial of Service Vulnerability

Popis

Vývojári antivírusového programu ClamAV vydali bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť v komponente *clamscan*.
Bezpečnostná zraniteľnosť je spôsobená nesprávnym spracovaním PDF súborov a umožňuje vzdialenému neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upraveného pdf súboru spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

26.04.2018

CVE

CVE-2018-0202

Zasiahnuté systémy

ClamAV v0.99.x a nižšie

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy a súbory z neznámych zdrojov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=57576