BEZPEČNOSTNÝ BULLETIN

Týždeň 10. 10. 2018 - 16. 10. 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-158

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 v procese spracovania JavaScriptu a umožňujú útočníkom vykonať škodlivý kód v kontexte privilegovaného procesu.

Dátum prvého zverejnenia varovania

02.10.2018

CVE

CVE-2018-12386, CVE-2018-12387

Zasiahnuté systémy

Mozilla Firefox verzie staršie ako 62.0.3
Mozilla Firefox ESR verzie staršie ako 60.2.2

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.mozilla.org/en-US/security/advisories/mfsa2018-24/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12386
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12387

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

Identifikátor

Open Ticket Request System viacero zraniteľnosti

Popis

Vývojári frameworku Open Ticket Request System vydali aktualizáciu svojho produktu, ktorá rieši viacero zraniteľností. Najvážnejšia bezpečnostná zraniteľnosť umožňuje vzdialenému autentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených URL odkazov spôsobiť eskaláciu svojich privilégií.

Dátum prvého zverejnenia varovania

15.10.2018

CVE

CVE-2018-14593, CVE-2018-16586, CVE-2018-16587

Zasiahnuté systémy

Open Ticket Request System OTRS verzie staršie ako 6.0.11, 5.0.30, 4.0.32

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://community.otrs.com/security-advisory-2018-03-security-update-for-otrs-framework/?lang=de
https://lists.debian.org/debian-lts-announce/2018/08/msg00021.html
https://nvd.nist.gov/vuln/detail/CVE-2018-14593
https://community.otrs.com/security-advisory-2018-04-security-update-for-otrs-framework/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.2
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Linux Kernel zraniteľnosť

Popis

Vývojári Linux Kernel vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť vo funkcii xenvif_set_hash_mapping.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov zasiahnutým systémom a umožňuje lokalnému útočníkovi prostredníctvom zasielania špeciálne upravených požiadaviek spôsobiť zápis mimo vyčlenenej pamäte a následnú eskaláciu privilégií a zneprístupnenie služby.

Dátum prvého zverejnenia varovania

15.10.2018

CVE

CVE-2018-15471

Zasiahnuté systémy

Linux Kernel staršie ako 4.18.14

Následky

Eskalácia privilégií, Zneprístupnenie služby, Neoprávnený prístup k citlivým údajom,

Odporúčania

Administrátorom zasiahnutých systémov odporúčame bezodkladne nainštalovať bezpečnostné aktualizácie.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=59013

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

Identifikátor

Directory Server - Enterprise Server Administration Web UI zraniteľnosť

Popis

Nesprávna manipulácia s neplatnou hodnotou parametra žiadosti HTTP Directory Serverom - spôsobí dereferenciu ukazovateľa NULL (CWE-476) a následné odmietnutie služby v dôsledku ukončenia procesu.

Dátum prvého zverejnenia varovania

12.10.2018

CVE

CVE-2018-12469

Zasiahnuté systémy

Micro Focus Enterprise Developer a Enterprise Server 2.3 Update 2 a staršie, 3.0 pred aktualizáciou opravy 12 a 4.0 pred aktualizáciou opravy 2

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://nvd.nist.gov/vuln/detail/CVE-2018-12469

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

Identifikátor

Centos Web Panel viacero zraniteľností

Popis

Zero day zraniteľnosť v CentOS-WebPanel.com (CWP) CentOS Web Panel verzie 0.9.8.480 umožňuje vzdialenému autentifikovanému útočníkovi vykonanie ľubovoľného príkazu pomocou špeciálnych znakov v admin/index.php v parametroch service_start, service_restart, service_fullstatus alebo service_stop.

Dátum prvého zverejnenia varovania

15.10.2018

CVE

CVE-2018-18322, CVE-2018-18323

Zasiahnuté systémy

Centos Web Panel 0.9.8.48

Následky

Vykonanie škodlivého kódu

Odporúčania

Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).
Tiež odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.

Zdroje

https://0day.today/exploit/31304
https://seccops.com/centos-web-panel-0-9-8-480-multiple-vulnerabilities/

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

Identifikátor

IBM FileNet Content Manager zraniteľnosť

Popis

Program je pri spracovávaní údajov XML zraniteľný voči útoku XML External Entity Injection (XXE). Vzdialený útočník by mohol zneužiť túto zraniteľnosť na získanie prístupu k citlivým informáciám a zahltenie pamäťových zdrojov.

Dátum prvého zverejnenia varovania

12.10.2018

CVE

CVE-2018-1844

Zasiahnuté systémy

IBM FileNet Content Manager 5.2.1 a 5.5.0

Následky

Neoprávnený prístup k citlivým údajom.

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www-01.ibm.com/support/docview.wss?uid=ibm10732755

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

Identifikátor

IBM WebSphere Application Server zraniteľnosť

Popis

V programe IBM WebSphere Application Server Admin Console bola odhalená zraniteľnosť, ktorá umožní vzdialenému útočníkovi prechádzať adresáre v systéme. Útočník by mohol prostredníctvom špeciálne vytvorenej požiadavky získať prístup k súborom v systéme.

Dátum prvého zverejnenia varovania

12.10.2018

CVE

CVE-2018-1770

Zasiahnuté systémy

IBM WebSphere Application Server 7.0, 8.0, 8.5, a 9.0

Následky

Neoprávnený prístup k citlivým údajom.

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www-01.ibm.com/support/docview.wss?uid=ibm10729521

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 5.7
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Management Console of BlackBerry

Popis

Spoločnosť BlackBerry vydala bezpečnostnú aktualizáciu na svoj produkt Management Console of UEM, ktorá opravuje bezpečnostnú zraniteľnosť spočívajúcu v nedostatočnej implementácii bezpečnostných mechanizmov. Zraniteľnosť umožňuje útočníkovi prostredníctvom súborov cookie získať prístup do systému a vykonávať v ňom neoprávnené zmeny.

Dátum prvého zverejnenia varovania

12.10.2018

CVE

CVE-2018-8890

Zasiahnuté systémy

BlackBerry UEM 12.8.0 a 12.8.1

Následky

Neoprávnený prístup do systému
Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://nvd.nist.gov/vuln/detail/CVE-2018-8890

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

Identifikátor

Palo Alto Networks PAN-OS zraniteľnosť

Popis

Webové rozhranie GlobalProtect Portal Login Page obsahuje zraniteľnosť typu XSS (Cross Site Scripting). Úspešné zneužitie tejto zraniteľnosti môže umožniť neautentifikovanému útočníkovi vykonať ľubovoľný JavaScript alebo podsunúť HTML.

Dátum prvého zverejnenia varovania

12.10.2018

CVE

CVE-2018-10141

Zasiahnuté systémy

Palo Alto Networks PAN-OS 8.1.3 a starších

Následky

Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://securityadvisories.paloaltonetworks.com/Home/Detail/134?AspxAutoDetectCookieSupport=1
https://nvd.nist.gov/vuln/detail/CVE-2018-10141

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

Identifikátor

Cloud Foundry CF Networking Release

Popis

Softvér Cloud Foundry CF Networking Release obsahuje zraniteľnosť typu SQL injection. Vzdialený autentifikovaný útočník s mTLS certifikátmi by mohol zadávať ľubovoľné SQL dopyty a získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

12.10.2018

CVE

CVE-2018-15755

Zasiahnuté systémy

Cloud Foundry CF-Networking, verzie 2.11.0 až 2.15.0,

Následky

Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.cloudfoundry.org/blog/cve-2018-15755/