BEZPEČNOSTNÝ BULLETIN

Týždeň 31. 01. 2018 – 06. 02. 2018

OBSAH BEZPEČNOSTNÉHO BULLETINU

Číslo	Identifikátor	Dôležitosť	CVSS Skóre
1	Mozilla Firefox Arbitrary code execution through unsanitized browser UI	Vysoká	**8.8**
2	Cisco Aggregation Services Router 9000 Series DoS Vulnerability	Vysoká	**8.6**
3	WordPress CMS Denial of Service Vulnerability	Vysoká	**7.5**
4	Fortify Audit Workbench and Software Security Center Vulnerability	Vysoká	**7.3**
5	Joomla! SQL and Cross-Site Scripting Vulnerabilities	Vysoká	**7.3**
6	EMC RecoverPoint Command Injection Vulnerabilities	Stredná	**6.7**
7	Django AuthenticationForm Information Disclosure Vulnerability	Stredná	**6.5**

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava

Mail: *sk-cert@nbu.gov.sk*
Mobil: *+421 903 993 706*
Tel: *+421 2 6869 2858*

SK-CERT
Naša značka:
02049/2018/TS/OKB-002

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

Identifikátor

Mozilla Firefox Arbitrary code execution through unsanitized browser UI

Popis

Spoločnosť Mozilla vydala aktualizáciu svojho internetového prehliadača Mozilla Firefox, ktorá rieši bezpečnostnú zraniteľnosť v používateľskom rozhraní prehliadača. Bezpečnostná zraniteľnosť umožňuje vzdialenému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s oprávneniami používateľa.

Dátum prvého zverejnenia varovania

29.01.2018

CVE

CVE-2018-5124

Zasiahnuté systémy

Mozilla Firefox verzie nižšie ako 58.0.1

Následky

Vykonanie škodlivého kódu

Odporúčania

Administrátorom zasiahnutých systémov odporúčame nainštalovať aktualizáciu uvedeného produktu.

Zdroje

https://www.mozilla.org/en-US/security/advisories/mfsa2018-05/
https://tools.cisco.com/security/center/viewAlert.x?alertId=56610
https://thehackernews.com/2018/01/firefox-browser-update.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.6**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Cisco Aggregation Services Router 9000 Series DoS Vulnerability

Popis

IPv6 podsystém operačného systému Cisco IOS XR Software Release 5.3.4 pre smerovače Cisco Aggregation Services Router (ASR) 9000 Series obsahuje zraniteľnosť, ktorú by vzdialený neautentifikovaný útočník mohol zneužiť na zneprístupnenie služby. Zraniteľnosť spočíva v nesprávnom spracovávaní IPv6 paketov s rozširujúcou hlavičkou Fragment Header a útočníkovi umožňuje vyvolať reštart jednej alebo viacerých linkových kariet Trident pripojených k smerovaču.

Dátum prvého zverejnenia varovania

31.01.2018 (posledná aktualizácia 03.02.2018)

CVE

CVE-2018-0136

Zasiahnuté systémy

Smerovače Cisco Aggregation Services Router (ASR) 9000 Series s operačným systémom Cisco IOS XR Software Release 5.3.4 a IPv6 konfigurovanými linkovými kartami Trident

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu uvedených produktov.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180131-ipv6
https://nvd.nist.gov/vuln/detail/CVE-2018-0136
https://www.securityfocus.com/bid/102905

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

Identifikátor

WordPress CMS Denial of Service Vulnerability

Popis

Populárny redakčný systém WordPress obsahuje zraniteľnosť, ktorú by vzdialený neautentifikovaný útočník mohol zneužiť na zneprístupnenie služby.
Zraniteľnosť spočíva v nesprávnej bezpečnostnej politike, ktorá neautentifikovaným útočníkom umožňuje volanie funkcie *load-scripts.php* určenej pre administrátorské rozhranie CMS systému. Opakovaným volaním skriptu so špecifickými vstupnými parametrami útočník môže postupne zahltiť dostupné systémové prostriedky servera a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

05.02.2018

CVE

CVE-2018-6389

Zasiahnuté systémy

CMS Wordpress po verziu 4.9.2

Následky

Zneprístupnenie služby

Odporúčania

Spoločnosť WordPress dosiaľ nevydala aktualizáciu riešiacu uvedenú zraniteľnosť.
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://thehackernews.com/2018/02/wordpress-dos-exploit.html
https://baraktawily.blogspot.sk/2018/02/how-to-dos-29-of-world-wide-websites.html

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

Identifikátor

Fortify Audit Workbench and Software Security Center Vulnerability

Popis

Produkty Fortify Audit Workbench a Software Security Center Vulnerability obsahujú zraniteľnosť, ktorú by vzdialený útočník mohol prostredníctvom XXE (XML External Entity) injekcie zneužiť na získanie prístupu k citlivým údajom.

Dátum prvého zverejnenia varovania

26.01.2018 (posledná aktualizácia 01.02.2018)

CVE

CVE-2018-6486

Zasiahnuté systémy

Micro Focus Fortify Audit Workbench (AWB) verzie 16.10, 16.20, 17.10
Micro Focus Fortify Software Security Center (SSC) verzie 16.10, 16.20, 17.10
HP Fortify Audit Workbench (AWB) verzie 16.10, 16.20, 17.10
HP Fortify Software Security Center (SSC) verzie 16.10, 16.20, 17.10

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu uvedených produktov.

Zdroje

https://softwaresupport.softwaregrp.com/document/-/facetsearch/document/KM03083653
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6486
https://www.securityfocus.com/bid/102902/

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

Identifikátor

Joomla! SQL and Cross-Site Scripting Vulnerabilities

Popis

Vývojári softvéru Joomla! vydali aktualizáciu svojho produktu, ktorá rieši viaceré bezpečnostné zraniteľnosti spôsobené nedostatočným overovaním vstupných údajov. Najvážnejšia bezpečnostná zraniteľnosť umožňuje vzdialenému útočníkovi prostredníctvom špeciálnych SQL príkazov získať prístup k citlivým údajom a vykonať príkazy v kontexte prihláseného používateľa.

Dátum prvého zverejnenia varovania

30.01.2018

CVE

CVE-2018-6376, CVE-2018-6377, CVE-2018-6379, CVE-2018-6380

Zasiahnuté systémy

Joomla! verzie staršie ako 3.8.4

Následky

Únik citlivých informácií, Neoprávnená zmena v systéme

Odporúčania

Administrátorom zasiahnutých systémov odporúčame nainštalovať aktualizáciu uvedeného produktu.

Zdroje

https://developer.joomla.org/security-centre/722-20180104-core-sqli-vulnerability.html
https://tools.cisco.com/security/center/viewAlert.x?alertId=56638
https://tools.cisco.com/security/center/viewAlert.x?alertId=56641
https://tools.cisco.com/security/center/viewAlert.x?alertId=56640
https://tools.cisco.com/security/center/viewAlert.x?alertId=56639

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 6.7**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

EMC RecoverPoint Command Injection Vulnerabilities

Popis

Spoločnosť EMC vydala aktualizáciu svojho produktu EMC RecoverPoint, ktorá rieši bezpečnostné zraniteľnosti spôsobené nedostatočným overovaním používateľských vstupov. Bezpečnostné zraniteľnosti umožňujú lokálnemu útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov získať eskalované privilégiá na napadnutom systéme.

Dátum prvého zverejnenia varovania

31.01.2018

CVE

CVE-2018-1184, CVE-2018-1185

Zasiahnuté systémy

EMC RecoverPoint for Virtual Machines verzie staršie ako 5.1.1
EMC RecoverPoint verzia 5.1.0.0 a staršie
EMC RecoverPoint verzie staršie ako 5.0.1.3

Následky

Eskalácia privilégií

Odporúčania

Administrátorom zasiahnutých systémov odporúčame nainštalovať aktualizáciu uvedeného produktu.

Zdroje

http://seclists.org/fulldisclosure/2018/Feb/9
https://tools.cisco.com/security/center/viewAlert.x?alertId=56660
https://tools.cisco.com/security/center/viewAlert.x?alertId=56661

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

Identifikátor

Django AuthenticationForm Information Disclosure Vulnerability

Popis

Vývojári webového frameworku Django vydali aktualizáciu svojho produktu, ktorá rieši bezpečnostnú zraniteľnosť spôsobenú nedostatočnou implementáciou bezpečnostnej politiky. Bezpečnostná zraniteľnosť umožňuje vzdialenému útočníkovi prostredníctvom funkcie *confirm_login_allowed* v procese *django.contrib.auth.forms.AuthenticationForm* vložiť nesprávne autentifikačné údaje. Tieto údaje však zraniteľný systém akceptuje a útočník tak môže získať prístup k citlivým údajom o používateľoch napadnutého systému.

Dátum prvého zverejnenia varovania

01.02.2018

CVE

CVE-2018-6188

Zasiahnuté systémy

Django master branch
Django verzie 2.0 a 2.0.1
Django verzie 1.11.8 a 1.11.9

Následky

Únik citlivých informácií

Odporúčania

Administrátorom zasiahnutých systémov odporúčame nainštalovať aktualizáciu uvedeného produktu.

Zdroje

https://www.djangoproject.com/weblog/2018/feb/01/security-releases/
http://www.vuxml.org/freebsd/d696473f-9f32-42c5-a106-bf4536fb1f74.html
https://tools.cisco.com/security/center/viewAlert.x?alertId=56659