BEZPEČNOSTNÝ BULLETIN

Týždeň 14. 03. 2018 – 20. 03. 2018

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	SAP Security Patch	Vysoká	**8.8**
02.	Kentico CMS Multiple Vulnerabilities	Vysoká	**8.8**
03.	Security updates available for Flash Player, Dreamweaver CC and Connect	Vysoká	**8.8**
04.	Mozilla Foundation Security Advisory	Vysoká	**8.8**
05.	VMware Workstation and Fusion VNC Session Handling Lets Remote Users Deny Service	Vysoká	**7.5**
06.	cURL Multiple Vulnerabilities	Vysoká	**7.5**
07.	Samba Releases Security Updates	Vysoká	**7.4**
08.	MikroTik RouterOS SMB Buffer Overflow Vulnerability	Vysoká	**7.3**

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-021

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

Identifikátor

SAP Security Patch

Popis

Spoločnosť SAP vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie zraniteľnosti by vzdialený neautentifikovaný útočník mohol prostredníctvom podvrhnutia špeciálne vytvorených súborov zneužiť na vykonanie škodlivého kódu.
Ďalšie zraniteľnosti spočívajúce v nedostatočnom overovaní používateľských vstupov by vzdialený útočník mohol zneužiť na realizáciu XSS (Cross-Site Scripting) útoku a v prípade jeho úspešnosti vykonať škodlivý JavaScript kód a získať prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

13.03.2018

CVE

CVE-2004-1308, CVE-2005-3350, CVE-2005-2974, CVE-2018-2402, CVE-2018-2400, CVE-2018-2398, CVE-2018-2399, CVE-2018-2397, CVE-2018-2401, CVE-2018-2369, CVE-2018-2366

Zasiahnuté systémy

SAP Internet Graphic Server verzie 7.20, 7.20_EXT, 7.45, 7.49, 7.53
SAP HANA verzie 1.00, 1.20, 2.00
SAP Business Process Automation (BPA) verzie 9.00, 9.10Samba Releases Security Updates
SAP Business Client verzie 6.5
SAP NetWeaver Business Warehouse verzie 7.00, 7.01, 7.02, 7.10, 7.11, 7.20, 7.30, 7.31, 7.40
SAP Business Objects Business Intelligence Platform 4.00, 4.10, 4.20, 4.30

Následky

Vykonanie škodlivého kódu, Neopravený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://blogs.sap.com/2018/03/13/sap-security-patch-day-march-2018/

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

Identifikátor

Kentico CMS Multiple Vulnerabilities

Popis

Spoločnosť Kentico vydala bezpečnostné aktualizácie na svoj produkt Kentico CMS, ktoré opravujú viacero bezpečnostných zraniteľností v administrátorskom rozhraní.
Najvážnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených webových odkazov spôsobiť vykonanie škodlivého kódu a narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

19.03.2018

CVE

CVE-2018-6842, CVE-2018-6843

Zasiahnuté systémy

Kentico CMS verzie 10.0 a 11.0

Následky

Vykonanie škodlivého kódu a narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://nvd.nist.gov/vuln/detail/CVE-2018-6842
https://nvd.nist.gov/vuln/detail/CVE-2018-6843
https://gist.github.com/zamous/c0afd7e21f3111de873c7bef6dcd9dd7

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

Identifikátor

Security updates available for Flash Player, Dreamweaver CC and Connect

Popis

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoje produkty Flash Player, Dreamweaver CC a Connect, ktoré opravujú viacero bezpečnostných zraniteľností.
Najvážnejšie bezpečnostné zraniteľnosti by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne upravených súborov (napr. ako príloha e-mailovej správy alebo škodlivý obsah webovej stránky) mohol zneužiť na vykonanie škodlivého kódu v kontexte prihláseného používateľa.

Dátum prvého zverejnenia varovania

13.03.2018

CVE

CVE-2018-4919, CVE-2018-4920, CVE-2018-4921, CVE-2018-4923, CVE-2018-4924

Zasiahnuté systémy

Adobe Flash Player verzia 28.0.0.161 a staršie
Adobe Connect verzia 9.7 a staršie
Adobe Dreamweaver CC verzia 18.0 a staršie

Následky

Vykonanie škodlivého kódu a narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých produktov. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://helpx.adobe.com/security/products/flash-player/apsb18-05.html
https://helpx.adobe.com/security/products/connect/apsb18-06.html
https://helpx.adobe.com/security/products/dreamweaver/apsb18-07.html
https://www.securitytracker.com/id/1040509
https://access.redhat.com/security/cve/cve-2018-4919
https://access.redhat.com/security/cve/cve-2018-4920

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

Identifikátor

Mozilla Foundation Security Advisory

Popis

Spoločnosť Mozilla vydala bezpečnostné aktualizácie, ktoré riešia 21 bezpečnostných zraniteľností v produktoch Firefox a Firefox ESR.
Najvážnejšie bezpečnostné zraniteľnosti by vzdialený neautentifikovaný útočník mohol zneužiť prostredníctvom podvrhnutia škodlivého webového obsahu na vykonanie škodlivého kódu a narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.03.2018 (posledná aktualizácia 16.03.2018)

CVE

CVE-2018-5125, CVE-2018-5126, CVE-2018-5127, CVE-2018-5128, CVE-2018-5129, CVE-2018-5130, CVE-2018-5131, CVE-2018-5132, CVE-2018-5133, CVE-2018-5134, CVE-2018-5135, CVE-2018-5136, CVE-2018-5137, CVE-2018-5138, CVE-2018-5140, CVE-2018-5141, CVE-2018-5142, CVE-2018-5143, CVE-2018-5145, CVE-2018-5146, CVE-2018-5147

Zasiahnuté systémy

Mozilla Firefox verzie staršie ako 59
Mozilla Firefox ESR verzie staršie ako 52.7

Následky

Vykonanie škodlivého kódu a narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom zasiahnutých systémov odporúčame bezodkladne nainštalovať bezpečnostné aktualizácie.

Zdroje

https://www.mozilla.org/en-US/security/advisories/mfsa2018-06/
https://www.mozilla.org/en-US/security/advisories/mfsa2018-07/

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

Identifikátor

VMware Workstation and Fusion VNC Session Handling Lets Remote Users Deny Service

Popis

Spoločnosť VMware vydala bezpečnostné aktualizácie na svoje produkty Workstation a Fusion, ktoré opravujú spoločnosťou bližšie nešpecifikovanú bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť umožňuje vzdialenému útočníkovi vytvorením viacerých VNC spojení spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

15.03.2018

CVE

CVE-2018-6957

Zasiahnuté systémy

Workstation verzie 14.x a 12.x
Fusion verzie 10.x a 8.x

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov. Administrátorom produktov VMware Workstation Pro 12.x a VMware Fusion 8.x odporúčame nastaviť autentifikačné heslo pre VNC spojenia, ktoré uvedenú zraniteľnosť eliminuje.

Zdroje

https://www.vmware.com/security/advisories/VMSA-2018-0008.html
https://kb.vmware.com/s/article/52934
https://securitytracker.com/id/1040539

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

Identifikátor

cURL Multiple Vulnerabilities

Popis

Vývojári produktu cURL vydali bezpečnostnú aktualizáciu, ktorá opravuje viaceré bezpečnostné zraniteľnosti.
Najvážnejšia bezpečnostná zraniteľnosť je zapríčinená vykonávaním nesprávnych pamäťových operácií v zasiahnutom systéme. Zraniteľnosť umožňuje vzdialenému útočníkovi prostredníctvom podvrhnutia špeciálne upravenej RTSP URL spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

14.03.2018

CVE

CVE-2018-1000120, CVE-2018-1000121, CVE-2018-1000122

Zasiahnuté systémy

cURL verzie nižšie ako 7.59.0

Následky

Vykonanie škodlivého kódu, Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://curl.haxx.se/docs/adv_2018-b047.html
https://curl.haxx.se/docs/adv_2018-9cd6.html
https://tools.cisco.com/security/center/viewAlert.x?alertId=57221
https://tools.cisco.com/security/center/viewAlert.x?alertId=57222

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

Identifikátor

Samba Releases Security Updates

Popis

Vývojári softvéru Samba vydali aktualizáciu svojho produktu, ktorá rieši bezpečnostné zraniteľnosti spôsobené nedostatočnou implementáciou bezpečnostných opatrení.
Najvážnejšia bezpečnostná zraniteľnosť umožňuje vzdialenému autentifikovanému útočníkovi prostredníctvom požiadaviek na LDAP server zmeniť používateľské a administrátorské prihlasovacie heslá.

Dátum prvého zverejnenia varovania

13.3.2018

CVE

CVE-2018-1050, CVE-2018-1057

Zasiahnuté systémy

Samba

Následky

Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://www.samba.org/samba/security/CVE-2018-1057.html
https://www.samba.org/samba/security/CVE-2018-1050.html
https://access.redhat.com/security/cve/cve-2018-1057

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

Identifikátor

MikroTik RouterOS SMB Buffer Overflow Vulnerability

Popis

Služba SMB v produkte Mikrotik RouterOS obsahuje bezpečnostnú zraniteľnosť, ktorú by vzdialený neautentifikovaný útočník mohol zneužiť na vyvolanie pretečenia zásobníka a následné vykonanie škodlivého kódu. Uvedená zraniteľnosť spočíva v nesprávnom parsovaní NetBIOS požiadaviek.

Dátum prvého zverejnenia varovania

15.03.2018

CVE

CVE-2018-7445

Zasiahnuté systémy

Zariadenia bežiace s RouterOS okrem verzií 6.41.3 a 6.42rc27

Následky

Vykonanie škodlivého kódu a narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.coresecurity.com/advisories/mikrotik-routeros-smb-buffer-overflow
https://www.securityfocus.com/bid/103427