BEZPEČNOSTNÝ BULLETIN

Týždeň 23. 10. 2019 - 29. 10. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Foxit PhantomPDF zraniteľnosti	Vysoká	**8.8**
02.	Mozilla Firefox a Thunderbird zraniteľnosti	Vysoká	**8.8**
03.	Google Chrome viacero zraniteľností	Vysoká	**8.8**
04.	WiKID Systems 2FA Enterprise Server viacero zraniteľností	Vysoká	**8.8**
05.	FusionPBX viacero zraniteľností	Vysoká	**8.8**
06.	Zraniteľnosti v Sitemagic CMS	Vysoká	**8.8**
07.	Trend Micro OfficeScan, Apex One a Worry-Free zraniteľnosti	Vysoká	**8.8**
08.	MikroTik RouterOS zraniteľnosti	Vysoká	**7.5**

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:
01380/2019/SK-CERT-259

BEZPEČNOSTNÝ BULLETIN

Týždeň 23. 10. 2019 - 29. 10. 2019

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

Identifikátor

Foxit PhantomPDF zraniteľnosti

Popis

Spoločnosť Foxit Software vydala bezpečnostnú aktualizáciu na svoj produkt Foxit PhantomPDF, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

16.10.2019

CVE

CVE-2019-17139, CVE-2019-17140, CVE-2019-17141, CVE-2019-17142, CVE-2019-17143, CVE-2019-17144, CVE-2019-17145

Zasiahnuté systémy

Foxit PhantomPDF verzie staršie ako 9.7

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.zerodayinitiative.com/advisories/ZDI-19-915/
https://www.zerodayinitiative.com/advisories/ZDI-19-909/
https://www.zerodayinitiative.com/advisories/ZDI-19-910/
https://www.zerodayinitiative.com/advisories/ZDI-19-911/
https://www.zerodayinitiative.com/advisories/ZDI-19-912/
https://www.zerodayinitiative.com/advisories/ZDI-19-913/
https://www.zerodayinitiative.com/advisories/ZDI-19-914/
https://www.zerodayinitiative.com/advisories/ZDI-19-914/
https://www.foxitsoftware.com/support/security-bulletins.php

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:
01380/2019/SK-CERT-259

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

Identifikátor

Mozilla Firefox a Thunderbird zraniteľnosti

Popis

Spoločnosť Mozilla vydala bezpečnostné aktualizácie na svoje produkty Firefox, Firefox ESR a Thunderbird, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

22.10.2019

CVE

CVE-2018-6156, CVE-2019-11757, CVE-2019-11758, CVE-2019-11759, CVE-2019-11760, CVE-2019-11761, CVE-2019-11762, CVE-2019-11763, CVE-2019-11764, CVE-2019-11765, CVE-2019-15903, CVE-2019-17000, CVE-2019-17001, CVE-2019-17002

Zasiahnuté systémy

Firefox verzie staršie ako 70
Firefox ESR verzie staršie ako 68.2
Thunderbird verzie staršie ako 68.2

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.mozilla.org/en-US/security/advisories/mfsa2019-33/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-34/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-35/
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-mozilla-firefox-could-allow-for-arbitrary-code-execution_2019-113/
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-mozilla-thunderbird-could-allow-for-arbitrary-code-execution_2019-115/
https://www.bleepingcomputer.com/news/software/firefox-70-released-with-in-browser-data-breach-notifications/

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

Identifikátor

Google Chrome viacero zraniteľností

Popis

Spoločnosť Google vydala aktualizáciu na svoj internetový prehliadač Google Chrome, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upraveného webového obsahu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

22.10.2019

CVE

CVE-2019-13699, CVE-2019-13700, CVE-2019-13701, CVE-2019-13702, CVE-2019-13703, CVE-2019-13704, CVE-2019-13705, CVE-2019-13706, CVE-2019-13707, CVE-2019-13708, CVE-2019-13709, CVE-2019-13710, CVE-2019-13711, CVE-2019-13713, CVE-2019-13714, CVE-2019-13715, CVE-2019-13716, CVE-2019-13717, CVE-2019-13718, CVE-2019-13719, CVE-2019-15903

Zasiahnuté systémy

Google Chrome verzie staršie ako 78

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://chromereleases.googleblog.com/2019/10/stable-channel-update-for-desktop_22.html
https://venturebeat.com/2019/10/22/google-chrome-78/
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-chrome-could-allow-for-arbitrary-code-execution_2019-114/
https://www.bleepingcomputer.com/news/software/chrome-78-released-with-doh-trial-tab-hover-cards-and-more/

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

Identifikátor

WiKID Systems 2FA Enterprise Server viacero zraniteľností

Popis

Spoločnosť WiKID Systems vydala aktualizáciu na svoj produkt 2FA Enterprise Server, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom SQL injection útoku vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

16.10.2019

CVE

CVE-2019-16917, CVE-2019-17114, CVE-2019-17115, CVE-2019-17116, CVE-2019-17117, CVE-2019-17118, CVE-2019-17119, CVE-2019-17120

Zasiahnuté systémy

WiKID Systems 2FA Enterprise Server verzie staršie ako 4.2.0.b2053

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.securitymetrics.com/blog/wikid-2fa-enterprise-server-sql-injection
https://seclists.org/fulldisclosure/2019/Oct/35
https://www.securitymetrics.com/blog/wikid-2fa-enterprise-server-cross-site-scripting
https://nvd.nist.gov/vuln/detail/CVE-2019-17117

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

Identifikátor

FusionPBX viacero zraniteľností

Popis

Vývojári produktu FusionPBX vydali bezpečnostnú aktualizáciu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti spočívajú v nedostatočnom overovaní používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

19.10.2019

CVE

CVE-2019-16968, CVE-2019-16969, CVE-2019-16970, CVE-2019-16971, CVE-2019-16972, CVE-2019-16973, CVE-2019-16974, CVE-2019-16975, CVE-2019-16978, CVE-2019-16979, CVE-2019-16980, CVE-2019-16981, CVE-2019-16982, CVE-2019-16983, CVE-2019-16984, CVE-2019-16986, CVE-2019-16987, CVE-2019-16988, CVE-2019-16989, CVE-2019-16990, CVE-2019-16991

Zasiahnuté systémy

FusionPBX 4.5.7

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Telefónne ústredne odporúčame prevádzkovať úplne odpojené od Internetu.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje
https://nvd.nist.gov/nvd.cfm?cvename=CVE-2019-16986
https://nvd.nist.gov/nvd.cfm?cvename=CVE-2019-16980
https://nvd.nist.gov/nvd.cfm?cvename=CVE-2019-16972
https://nvd.nist.gov/nvd.cfm?cvename=CVE-2019-16979
https://nvd.nist.gov/nvd.cfm?cvename=CVE-2019-16971
https://nvd.nist.gov/nvd.cfm?cvename=CVE-2019-16970
https://nvd.nist.gov/nvd.cfm?cvename=CVE-2019-16969
https://nvd.nist.gov/nvd.cfm?cvename=CVE-2019-16968
https://nvd.nist.gov/nvd.cfm?cvename=CVE-2019-16974
https://nvd.nist.gov/nvd.cfm?cvename=CVE-2019-16975
https://nvd.nist.gov/nvd.cfm?cvename=CVE-2019-16978
https://nvd.nist.gov/nvd.cfm?cvename=CVE-2019-16973
https://nvd.nist.gov/nvd.cfm?cvename=CVE-2019-16981
https://nvd.nist.gov/nvd.cfm?cvename=CVE-2019-16990
https://nvd.nist.gov/nvd.cfm?cvename=CVE-2019-16983
https://nvd.nist.gov/nvd.cfm?cvename=CVE-2019-16984
https://nvd.nist.gov/nvd.cfm?cvename=CVE-2019-16987
https://nvd.nist.gov/nvd.cfm?cvename=CVE-2019-16988
https://nvd.nist.gov/nvd.cfm?cvename=CVE-2019-16989
https://nvd.nist.gov/nvd.cfm?cvename=CVE-2019-16991
https://nvd.nist.gov/nvd.cfm?cvename=CVE-2019-16982

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

Identifikátor

Zraniteľnosti v Sitemagic CMS

Popis

Vývojári redakčného systému Sitemagic CMS vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom Cross-Site-Request-Forgery (CSRF) útoku vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

18.10.2019

CVE

CVE-2019-18220

Zasiahnuté systémy

Sitemagic CMS verzie staršie ako 4.4.2

Následky

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

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky nie sú založené na redakčnom systéme Sitemagic v zraniteľných verziách. V prípade že áno, zabezpečte aktualizáciu redakčného systému.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://github.com/Jemt/SitemagicCMS/commit/a6e77e0d834508b5775e71ec1aa166a63e44eb1c
https://nvd.nist.gov/vuln/detail/CVE-2019-18220

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

Identifikátor

Trend Micro OfficeScan, Apex One a Worry-Free zraniteľnosti

Popis

Spoločnosť Trend Micro vydala bezpečnostné aktualizácie na svoje produkty OfficeScan, Apex One a Worry-Free, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Zraniteľnosť je v súčasnosti aktívne zneužívaná útočníkmi.

Dátum prvého zverejnenia varovania

28.10.2019

CVE

CVE-2019-18187, CVE-2019-18188, CVE-2019-18189

Zasiahnuté systémy

Trend Micro OfficeScan verzie staršie ako XG SP1 CP 5427, XG CP 1962 a 11.0 SP1 CP 6638
Trend Micro Apex One verzie staršie ako CP 2049
Trend Micro Worry-Free Business Security verzie staršie ako 10.0 SP1 Patch 2178, 10.0 Patch 1569 a 9.5 CP 1513

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://success.trendmicro.com/solution/000151732
https://success.trendmicro.com/solution/000151730
https://success.trendmicro.com/solution/000151731
https://nvd.nist.gov/vuln/detail/CVE-2019-18189
https://nvd.nist.gov/vuln/detail/CVE-2019-18187
https://nvd.nist.gov/vuln/detail/CVE-2019-18188

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

Identifikátor

MikroTik RouterOS zraniteľnosti

Popis

Spoločnosť MikroTik vydala bezpečnostnú aktualizáciu RouterOS, ktorá opravuje zraniteľnosti svojich routerov .
Bezpečnostné zraniteľnosti sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov a umožňujú vzdialenému, neautentifikovanému útočníkovi vykonávať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

28.10.2019

CVE

CVE-2019-3976, CVE-2019-3977, CVE-2019-3978, CVE-2019-3979

Zasiahnuté systémy

MikroTik RouterOS verzie staršie ako 6.45.7, 6.44.6, 6.46beta59

Následky

Neoprávnený prístup do systému
Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://blog.mikrotik.com/security/dns-cache-poisoning-vulnerability.html
https://blog.mikrotik.com/security/package-validation-and-upgrade-vulnerability.html
https://www.tenable.com/security/research/tra-2019-46