BEZPEČNOSTNÝ BULLETIN

Týždeň 03. 06. 2020 - 09. 06. 2020

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Mozilla Firefox viacero zraniteľností	Vysoká	**8.8**
02.	Google Chrome viacero zraniteľností	Vysoká	**8.8**
03.	Vivotek IP kamery zraniteľnosti	Vysoká	**8.8**
04.	Aruba ClearPass Policy Manager zraniteľnosti	Vysoká	**8.1**
05.	FortiClient zraniteľnosť	Vysoká	**7.8**
06.	Django framework zraniteľnosti	Vysoká	**7.5**
07.	PACTware zraniteľnosti	Vysoká	**7.1**

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:
01439/2020/SK-CERT-138

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 na svoje produkty Firefox a Firefox ESR, ktoré opravujú viacero bezpečnostných zraniteľností.
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

02.06.2020

CVE

CVE-2020-12399, CVE-2020-12405, CVE-2020-12406, CVE-2020-12407, CVE-2020-12408, CVE-2020-12409, CVE-2020-12410, CVE-2020-12411

Zasiahnuté systémy

Firefox verzie staršie ako 77
Firefox ESR verzie staršie ako 68.9

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/mfsa2020-21/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-20/
https://exchange.xforce.ibmcloud.com/vulnerabilities/182802
https://exchange.xforce.ibmcloud.com/vulnerabilities/182799
https://exchange.xforce.ibmcloud.com/vulnerabilities/182805

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 chýb a 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

03.06.2020

CVE

CVE-2020-6493, CVE-2020-6494, CVE-2020-6495, CVE-2020-6496, CVE-2020-6497, CVE-2020-6498

Zasiahnuté systémy

Google Chrome verzie staršie ako 83.0.4103.97

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/2020/06/stable-channel-update-for-desktop.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/182831
https://exchange.xforce.ibmcloud.com/vulnerabilities/182827

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

Identifikátor

Vivotek IP kamery zraniteľnosti

Popis

Spoločnosť Vivotek vydala bezpečnostné aktualizácie na svoje IP kamery, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bližšie nešpecifikovaná bezpečnostná zraniteľnosť umožňuje vzdialenému, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

26.05.2020

CVE

CVE-2020-11949, CVE-2020-11950

Zasiahnuté systémy

Vivotek IP kamery s firmvérom starším ako XXXXX-VVTK-2.2002.xx.01x a XXXXX-VVTK-0XXXX_Beta2

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne 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

http://download.vivotek.com/downloadfile/support/cyber-security/vvtk-sa-2020-001-v1.pdf
https://nvd.nist.gov/vuln/detail/CVE-2020-11949
https://nvd.nist.gov/vuln/detail/CVE-2020-11950

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.1**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Aruba ClearPass Policy Manager zraniteľnosti

Popis

Spoločnosť Aruba Networks vydala bezpečnostné aktualizácie na svoj produkt ClearPass Policy Manager, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť vo webovom rozhraní umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

02.06.2020

CVE

CVE-2020-7115, CVE-2020-7116, CVE-2020-7117

Zasiahnuté systémy

ClearPass Policy Manager verzie staršie ako 6.9.1, 6.8.5-HF, 6.8.6 a 6.7.13-HF

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne 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.arubanetworks.com/assets/alert/ARUBA-PSA-2020-005.txt

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

Identifikátor

FortiClient zraniteľnosť

Popis

Spoločnosť Fortinet vydala aktualizáciu na svoj produkt FortiClient, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá.

Dátum prvého zverejnenia varovania

25.05.2020

CVE

CVE-2020-9291

Zasiahnuté systémy

FortiClient for Windows verzie staršie ako 6.2.1

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://fortiguard.com/psirt/FG-IR-20-040
https://nvd.nist.gov/vuln/detail/CVE-2020-9291

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

Identifikátor

Django framework zraniteľnosti

Popis

Vývojári webového frameworku Django vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

03.06.2020

CVE

CVE-2020-13254, CVE-2020-13596

Zasiahnuté systémy

Django verzie staršie ako 3.1, 3.0 a 2.2

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Odporúčame uistiť sa, či Vaše webové aplikácie nie sú založené na frameworku Django v zraniteľných verziách. V prípade, že áno, vykonajte aktualizáciu frameworku.
Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.djangoproject.com/weblog/2020/jun/03/security-releases/
https://nvd.nist.gov/vuln/detail/CVE-2020-13254
https://nvd.nist.gov/vuln/detail/CVE-2020-13596

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

Identifikátor

PACTware zraniteľnosti

Popis

Spoločnosť PACTware vydala bezpečnostnú aktualizáciu na svoj produkt PACTware, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov a umožňujú lokálnemu, autentifikovanému útočníkovi vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

29.05.2020

CVE

CVE-2020-9403, CVE-2020-9404

Zasiahnuté systémy

PACTware verzie staršie ako 5.0.5.31 a 4.1 SP6

Následky

Neoprávnený prístup do systému
Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame kontaktovať dodávateľa a vykonať aktualizáciu zasiahnutých systémov. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://cert.vde.com/en-us/advisories/vde-2020-017