BEZPEČNOSTNÝ BULLETIN

Týždeň 06. 05. 2020 - 12. 05. 2020

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	vBulletin zraniteľnosť	Vysoká	**8.8**
02.	Mozilla Firefox viacero zraniteľností	Vysoká	**8.8**
03.	Symantec Endpoint Protection zraniteľnosti	Vysoká	**7.8**
04.	McAfee Endpoint produkty zraniteľnosti	Vysoká	**7.8**
05.	Dell OS recovery image zraniteľnosť	Vysoká	**7.8**
06.	Fazecast jSerialComm zraniteľnosť	Vysoká	**7.8**
07.	Citrix ShareFile StorageZones Controller viacero zraniteľností	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:
01439/2020/SK-CERT-111

BEZPEČNOSTNÝ BULLETIN

Týždeň 06. 05. 2020 - 12. 05. 2020

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

Identifikátor

vBulletin zraniteľnosť

Popis

Vývojári diskusného fóra vBulletin vydali aktualizáciu svojho produktu, ktorá opravuje bližšie nešpecifikovanú bezpečnostnú zraniteľnosť.
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.

Dátum prvého zverejnenia varovania

07.05.2020

CVE

-

Zasiahnuté systémy

vBulletin verzie staršie ako 5.6.1 Patch Level 1, 5.6.0 Patch Level 1 a 5.5.6 Patch Level 1

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://thehackernews.com/2020/05/vBulletin-access-vulnerability.html
https://www.tenable.com/blog/cve-2020-12720-vbulletin-urges-users-to-patch-undisclosed-security-vulnerability
https://forum.vbulletin.com/forum/vbulletin-announcements/vbulletin-announcements_aa/4440032-vbulletin-5-6-1-security-patch-level-1

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

05.05.2020

CVE

CVE-2020-12387, CVE-2020-12388, CVE-2020-12389, CVE-2020-12390, CVE-2020-12391, CVE-2020-12392, CVE-2020-12393, CVE-2020-12394, CVE-2020-12395, CVE-2020-12396, CVE-2020-6831

Zasiahnuté systémy

Firefox verzie staršie ako 76
Firefox ESR verzie staršie ako 68.8

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.cisecurity.org/advisory/multiple-vulnerabilities-in-mozilla-firefox-could-allow-for-remote-code-execution_2020-061/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-17/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-16/

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

Identifikátor

Symantec Endpoint Protection zraniteľnosti

Popis

Spoločnosť Symantec vydala bezpečnostnú aktualizáciu na svoj produkt Endpoint Protection, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá na zasiahnutom systéme.

Dátum prvého zverejnenia varovania

11.05.2020

CVE

CVE-2020-5833, CVE-2020-5834, CVE-2020-5835, CVE-2020-5836, CVE-2020-5837

Zasiahnuté systémy

Symantec Endpoint Protection verzie staršie ako 14.3
Symantec Endpoint Protection Manager verzie staršie ako 14.3

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.broadcom.com/security-advisory/security-advisory-detail.html?notificationId=SYMSA1762

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

Identifikátor

McAfee Endpoint produkty zraniteľnosti

Popis

Spoločnosť McAfee vydala bezpečnostné aktualizácie na svoje produkty EDR, MAR a MVISION, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov a umožňujú lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá.

Dátum prvého zverejnenia varovania

07.05.2020

CVE

CVE-2020-7285, CVE-2020-7286, CVE-2020-7287, CVE-2020-7288, CVE-2020-7289, CVE-2020-7290, CVE-2020-7291

Zasiahnuté systémy

MVISION Endpoint verzie staršie ako 20.5.0.94
McAfee Endpoint Detection and Response (EDR) client verzie staršie ako 3.1.0 Hotfix 1
McAfee Active Response (MAR) client verzie staršie ako 2.4.3 Hotfix 1

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://kc.mcafee.com/corporate/index?page=content&id=SB10317

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

Identifikátor

Dell OS recovery image zraniteľnosť

Popis

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

Dátum prvého zverejnenia varovania

05.05.2020

CVE

CVE-2020-5343

Zasiahnuté systémy

Dell OS recovery image stiahnuté pred 20.12.2019

Následky

Eskalácia privilégií
Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.dell.com/support/article/sk-sk/SLN321036
https://nvd.nist.gov/vuln/detail/CVE-2020-5343

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

Identifikátor

Fazecast jSerialComm zraniteľnosť

Popis

Spoločnosť Fazecast vydala bezpečnostnú aktualizáciu na svoj produkt jSerialComm, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

05.05.2020

CVE

CVE-2020-10626

Zasiahnuté systémy

Fazecast jSerialComm verzie staršie ako 2.2.2
Schneider Electric EcoStruxure IT Gateway 1.5.x, 1.6.x, 1.7.x

Následky

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

Odporúčania

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

Zdroje

https://www.us-cert.gov/ics/advisories/ICSA2012601
https://www.zerodayinitiative.com/advisories/ZDI-20-588/

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

Identifikátor

Citrix ShareFile StorageZones Controller viacero zraniteľností

Popis

Spoločnosť Citrix vydala aktualizáciu na svoj produkt ShareFile StorageZones Controller, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

05.05.2020

CVE

CVE-2020-7473, CVE-2020-8982, CVE-2020-8983

Zasiahnuté systémy

Citrix Storage Zones Controller verzie staršie ako 5.10.0, 5.9.1, 5.8.1 a 5.7.1
Citrix ShareFile StorageZones Controller verzie staršie ako 5.5.1 a 5.6.1

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. 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://support.citrix.com/article/CTX269106
https://thehackernews.com/2020/05/citrix-sharefile-vulnerability.html
https://nvd.nist.gov/vuln/detail/CVE-2020-8983
https://nvd.nist.gov/vuln/detail/CVE-2020-8982
https://nvd.nist.gov/vuln/detail/CVE-2020-7473