BEZPEČNOSTNÝ BULLETIN

Týždeň 20. 12. 2017 – 26. 12. 2017

OBSAH BEZPEČNOSTNÉHO BULLETINU

Číslo	Identifikátor	Dôležitosť	CVSS Score
1	IBM Financial Transaction Manager vulnerable to SQL injection	Vysoká	**8.8**
2	F5 BIG-IP multiple vulnerabilities	Vysoká	**7.9**
3	Dell EMC Data Domain SMBv1 Memory Overflow Remote Arbitrary Code Execution Vulnerability	Vysoká	**7.5**
4	QNAP QTS Multiple Vulnerabilities	Vysoká	**7.5**
5	Trend Micro Smart Protection Server (Standalone) Multiple Vulnerabilities	Vysoká	**7.4**
6	Mozilla Thunderbird Multiple Vulnerabilities	Vysoká	**7.3**
7	Massive cryptomining campaign targeting WordPress sites	Vysoká	-
8	Backdoor in Captcha Plugin Affects Multiple Wordpress Sites	Vysoká	-
9	Multiple vulnerabilities in Bitdefender	Stredná	**6.8**

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:
06282/2017/SKB/OBPr-038

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

Identifikátor

IBM Financial Transaction Manager vulnerable to SQL injection

Popis

Produkt IBM Financial Transaction Manager obsahuje zraniteľnosť typu SQL injekcia. Vzdialený útočník by mohol prostredníctvom špeciálne vytvorenej správy, obsahujúcej SQL, zobraziť, pridať, upraviť alebo odstrániť údaje v backend databáze.

Dátum prvého zverejnenia varovania

11.12.2017 (posledná aktualizácia 26.12.2017)

CVE

CVE-2017-1606

Zasiahnuté systémy

IBM Financial Transaction Manager (FTM) for Multi-Platform (MP) verzie 3.0.0.0 až 3.0.0.7

Následky

Neoprávnený prístup k údajom, Neoprávnená modifikácia údajov

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu dotknutého softvéru. Po vykonaní aktualizácie odporúčame preveriť integritu databázy a prístupové logy na prítomnosť pokusov o SQL injekciu.

Zdroje

https://nvd.nist.gov/vuln/detail/CVE-2017-1606

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.9**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

F5 BIG-IP multiple vulnerabilities

Popis

Spoločnosť F5 vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú viacero bezpečnostných zraniteľností.
Najvážnejšia je bezpečnostná zraniteľnosť v F5 BIG-IP, ktorá umožňuje vzdialenému útočníkovi pomocou paketov odosielaných na Virtual Server s klientskymi alebo serverovými SSL profilmi používajúcimi AES-GCM šifrovanie spôsobiť odopretie služieb.

Dátum prvého zverejnenia varovania

19.12.2017 (posledná aktualizácia 22.12.2017)

CVE

BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, GTM, Link Controller, PEM, WebSafe) 11; 12; 13
BIG-IP platforms: 2000s, 2200s, 4000s, 4200v, i5600, i5800, i7600, i7800, i10600, i10800, VIPRION 4450 blade

Zasiahnuté systémy

CVE-2017-0304, CVE-2017-6129, CVE-2017-6132, CVE-2017-6133, CVE-2017-6134, CVE-2017-6135, CVE-2017-6136, CVE-2017-6138, CVE-2017-6139, CVE-2017-6140, CVE-2017-6146, CVE-2017-6151, CVE-2017-6164, CVE-2017-6166, CVE-2017-6167

Následky

Neoprávnený zásah do systému, Odopretie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://support.f5.com/csp/article/K39428424
https://support.f5.com/csp/article/K43322910
https://support.f5.com/csp/article/K55102452
https://support.f5.com/csp/article/K24465120
https://www.securitytracker.com/id/1040041
https://www.securitytracker.com/id/1040042

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

Identifikátor

Dell EMC Data Domain SMBv1 Memory Overflow Remote Arbitrary Code Execution Vulnerability

Popis

Bezpečnostná zraniteľnosť v produktoch Dell EMC Data Domain umožňuje neautentifikovanému, vzdialenému útočníkovi vykonať škodlivý kód a spôsobiť odopretie služby.
Útočník môže posielaním vytvorených SMBv1 paketov spôsobiť pretečenie zásobníka a následne vykonať škodlivý kód, alebo spôsobiť odopretie služby zablokovaním SMB služby a autentifikácie Active Directory.

Dátum prvého zverejnenia varovania

20.12.2017

CVE

CVE-2017-14385

Zasiahnuté systémy

Data Domain DD OS 5.7;6.0; 6.1
Data Domain Virtual Edition 2.0; 3.0; 3.1

Následky

Neoprávnené vykonanie kódu, Odopretie služieb

Odporúčania

Administrátorom odporúčame bezodkladne vykonať štandardnú aktualizáciu zasiahnutých produktov a tiež zvážiť implementáciu zoznamu IP adries pre riadenie prístupu ACL.

Zdroje

http://seclists.org/fulldisclosure/2017/Dec/79
https://tools.cisco.com/security/center/viewAlert.x?alertId=56304

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

Identifikátor

QNAP QTS Multiple Vulnerabilities

Popis

Vybrané verzie QNAP QTS obsahujú zraniteľnosti, ktoré by vzdialený útočník mohol zneužiť na vyvolanie pretečenia zásobníka a následnému vykonaniu ľubovoľného kódu na zariadeniach NAS.

Dátum prvého zverejnenia varovania

15.12.2017 (posledná aktualizácia 21.12.2017)

CVE

CVE-2017-17027, CVE-2017-17028, CVE-2017-17029, CVE-2017-17030, CVE-2017-17031, CVE-2017-17032, CVE-2017-17033

Zasiahnuté systémy

QNAP QTS verzie 4.2.6 build 20171026, 4.3.3.0378 build 20171117, 4.3.4.0387 (Beta 2) build 20171116

Následky

Neoprávnené vykonanie kódu

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu QTS.

Zdroje

https://www.qnap.com/zh-tw/security-advisory/nas-201712-15

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

Identifikátor

Trend Micro Smart Protection Server (Standalone) Multiple Vulnerabilities

Popis

V administrátorskom rozhraní softvéru Smart Protection Server bolo objavených viacero zraniteľností. Najvážnejšia zraniteľnosť umožňuje vzdialenému útočníkovi získať prístup k diagnostickým záznamom aplikácie bez autentifikácie cez HTTPS, prevziať kontrolu nad reláciou používateľa a vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

19.12.2017

CVE

CVE-2017-11398, CVE-2017-14094, CVE-2017-14095, CVE-2017-14096, CVE-2017-14097

Zasiahnuté systémy

Smart Protection Server verzie nižšie ako 3.3, platforma Linux

Následky

Eskalácia privilégií, Neoprávnené vykonanie kódu, Únik citlivých informácií

Odporúčania

Používateľom a administrátorom odporúčame bezodkladne vykonať aktualizáciu dotknutých systémov.

Zdroje

https://success.trendmicro.com/solution/1118992
http://www.securityweek.com/code-execution-flaws-found-trend-micro-smart-protection-server

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

Identifikátor

Mozilla Thunderbird Multiple Vulnerabilities

Popis

Produkt Mozilla Thunderbird obsahuje viacero zraniteľností, ktoré by útočník mohol zneužiť na neoprávnený prístup k informáciám alebo odopretie služby.
Pri vykresľovaní elementov s knižnicou ANGLE prostredníctvom Direct 3D 9 dochádza k pretečeniu zásobníka, ktorým by útočník mohol spôsobiť pád aplikácie (zraniteľnosť sa týka len OS Windows). V parsovanom RSS feed-e je pri jeho zobrazení možné vykonať JavaScript kód. CSS so špecifickým formátom možno v RSS feed-e zneužiť na odhalenie používateľského mena. RSS polia môžu prostredníctvom injekcie modifikovať telo e-mailovej správy.

Dátum prvého zverejnenia varovania

22.12.2017

CVE

CVE-2017-7845, CVE-2017-7846, CVE-2017-7847, CVE-2017-7848

Zasiahnuté systémy

Mozilla Thunderbird 52.5.2

Následky

Odopretie služby, Neoprávnený prístup k informáciám

Odporúčania

Používateľom odporúčame bezodkladne vykonať aktualizáciu.

Zdroje

https://www.securityfocus.com/bid/102258/info
https://www.mozilla.org/en-US/security/advisories/mfsa2017-30/

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

Identifikátor

Massive cryptomining campaign targeting WordPress sites

Popis

V priebehu dňa 19.12.2017 bezpečnostní experti z WordFence detegovali masívnu vlnu brute force útokov cielených na webové stránky bežiace na platforme WordPress a predpokladajú, že na realizáciu útoku bola použitá jediná botnet sieť, pre ktorú sa podarilo identifikovať 8 riadiacich C&C serverov. Hlavným cieľom útoku bolo infikovať servery malwarom.

Útočník využíva sofistikovaný malware (variantu *Tsunami* alebo *Kaiten*) na vzdialené riadenie WordPress serverov. To umožňuje zneužitie kompromitovaných serverov ako prostriedok útoku voči iným WordPress stránkam a na aktívne ťaženie kryptomeny Monero, ktorú je možné efektívne ťažiť aj prostredníctvom hardvéru webových serverov. Útočníkom sa podarilo vyťažiť kryptomenu v približnej hodnote 100 000$.

Dátum prvého zverejnenia varovania

19.12.2017 (posledná aktualizácia 21.12.2017)

Zasiahnuté systémy

CMS WordPress

Následky

Botnet, Neprístupnosť služby

Odporúčania

Administrátorom CMS Wordpress odporúčame vykonať nasledovný postup:

1. Vykonať sken na PHP malware prostredníctvom služby alebo pluginu Wordfence.
2. Ak je to možné, vykonať kontrolu zaťaženia CPU serverov.
3. Zvýšiť odolnosť stránky voči brute-force útokom.
4. Monitorovať blacklisty (v prípade, že je Vaša stránka infikovaná, bude zaradená do blacklistov)
5. V prípade kompromitácie urýchlene vykonať obnovu zo zálohy.

Odolnosť voči brute-force možno zvýšiť napr.:

- inštaláciou firewallu Wordfence, ktorý blokuje brute force útoky.
- kontrolou dodržiavania bezpečnostnej politiky používania dostatočne komplexných hesiel pre používateľské a administrátorské účty.
- aktiváciou dvojfaktorovej autentifikácie na administrátorských účtoch.
- blokovaním spojení s IP adresami z blacklistu získaného počas uvedeného útoku.

- monitorovaním neúspešných pokusov o prihlásenie do systému so zasielaním alarmov administrátorom.

Zdroje
https://www.bleepingcomputer.com/news/security/massive-brute-force-attack-infects-wordpress-sites-with-monero-miners/ https://www.wordfence.com/blog/2017/12/massive-cryptomining-campaign-wordpress/ https://www.wordfence.com/blog/2017/12/aggressive-brute-force-wordpress-attack/

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

Identifikátor

Backdoor in Captcha Plugin Affects Multiple Wordpress Sites

Popis

Populárny plugin *„Captcha plugin“* od vývojára *Simplywordpress*, s viac ako 300 tisíc aktívnymi inštaláciami, bol odstránený z repozitára WordPress. Podľa vývojárov išlo o problémy spojené s názvom produktu.

Bezpečnostní experti z WordFence aktívne sledujú pluginy s veľkou používateľskou základňou, ktoré sú odstránené z repozitára. Bezpečnostný audit uvedeného pluginu odhalil kód, ktorý pri automatickej aktualizácii pluginu stiahne jeho kópiu v *zip* z webu simplywordpress.net a preinštaluje aktívnu verziu pluginu. Nová verzia obsahuje drobné zmeny v zdrojovom kóde a súbor *plugin-update.php* predstavuje backdoor, ktorý umožňuje neautorizovaný prístup do administrátorského rozhrania webu.

Experti z WordFence a plugin tím WordPress.org vytvorili novú verziu pluginu 4.4.5, ktorá odstraňuje backdoor funkcionalitu.

Dátum prvého zverejnenia varovania

19.12.2017 (posledná aktualizácia 21.12.2017)

Zasiahnuté systémy

CMS WordPress

Následky

Backdoor

Odporúčania

Administrátorom CMS Wordpress odporúčame uvedený Captcha plugin bezodkladne odinštalovať alebo vykonať jeho aktualizáciu na bezpečnú verziu 4.4.5, ktorú vytvoril tím WordFence. Odporúčame tiež aktivovať automatické aktualizácie systému WordPress.

Zdroje

https://www.wordfence.com/blog/2017/12/backdoor-captcha-plugin/
https://www.pluginvulnerabilities.com/tag/simplywordpress/

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 6.8**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Multiple vulnerabilities in Bitdefender

Popis

Produkt Bitdefender Internet Security 2018 obsahuje viacero zraniteľností, ktoré by vzdialený útočník mohol zneužiť na vykonanie škodlivého kódu. Útočný vektor vyžaduje interakciu používateľa, ktorý musí navštíviť škodlivú stránku alebo otvoriť škodlivý súbor. Nesprávne ošetrenie používateľských vstupov v *cevakrnl.xmd* môže vyvolať pretečenie zásobníka, ktoré útočník môže zneužiť na vykonanie kódu v kontexte SYSTEM.

Dátum prvého zverejnenia varovania

12.12.2017 (posledná aktualizácia 21.12.2017)

CVE

CVE-2017-17408, CVE-2017-17409, CVE-2017-17410

Zasiahnuté systémy

Bitdefender Internet Security 2018

Následky

Neoprávnené vykonanie kódu

Odporúčania

Administrátorom a používateľom odporúčame bezodkladne vykonať aktualizáciu dotknutých produktov.

Zdroje

http://zerodayinitiative.com/advisories/ZDI-17-942/
http://zerodayinitiative.com/advisories/ZDI-17-943/
http://zerodayinitiative.com/advisories/ZDI-17-944/