BEZPEČNOSTNÝ BULLETIN

Týždeň 27. 12. 2017 – 02. 01. 2018

OBSAH BEZPEČNOSTNÉHO BULLETINU

Číslo	Identifikátor	Dôležitosť	CVSS Score
1	Trustwave Secure Web Gateway Vulnerability	Vysoká	8.8
2	FortiClient improper access control of users' VPN credentials	Vysoká	8.8
3	Foxit Reader Multiple Vulnerabilities	Vysoká	8.8
4	IOHIDeous - Unpatched macOS Flaw Allows Code Execution, Root Access	Vysoká	8.4
5	IBM Tivoli Monitoring Remote Code Execution Vulnerability	Vysoká	8.0
6	Multiple Vulnerabilities in Qt for Android	Vysoká	7.5
7	Wordpres plugins hiding a backdoor	Vysoká	-
8	Samsung Internet Browser SOP Bypass/UXSS	Stredná	6.8
9	Synology Chat Multiple Vulnerabilities	Stredná	6.4

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:
00099/2018/SKB/OBPr-039

BEZPEČNOSTNÝ BULLETIN

Týždeň 27. 12. 2017 – 02. 01. 2017

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

Identifikátor

Trustwave Secure Web Gateway Vulnerability

Popis

Trustwave Secure Web Gateway obsahuje zraniteľnosť, ktorú by vzdialený útočník mohol zneužiť na pridanie verejného kľúča do zoznamu autorizovaných SSH kľúčov zariadenia (SSH Authorized Keys data), prostredníctvom parametra *publicKey* na URI */sendKey* metódou POST. Týmto postupom je možné získať prístupové oprávnenia úrovne root.

Dátum prvého zverejnenia varovania

31.12.2017

CVE

CVE-2017-18001

Zasiahnuté systémy

Trustwave Secure Web Gateway (SWG) po verziu 11.8.0.27

Následky

Neoprávnený prístup do systému, Eskalácia privilégií

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu a limitovať prístup k systému SWG na základe IP adresy zavedením ACL zoznamu pre riadenie prístupov.

Zdroje

http://seclists.org/fulldisclosure/2017/Dec/88
https://www.trustwave.com/Resources/Trustwave-Software-Updates/Important-Security-Update-for-Trustwave-Secure-Web-Gateway/
https://blogs.securiteam.com/index.php/archives/3550

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

Identifikátor

FortiClient improper access control of users' VPN credentials

Popis

Produkt FortiClient obsahuje zraniteľnosť, ktorú by útočník mohol zneužiť na získanie šifrovacích kľúčov použitých na zabezpečenie autentifikačných údajov pre VPN.
Ak je aktivovaná funkcia "Save Pasword" použitá používateľom, FortiClient ukladá autentifikačné údaje pre VPN v šifrovanej podobe na nezabezpečených miestach. Z binárnych súborov je následne možné extrahovať šifrovací kľúč.

Dátum prvého zverejnenia varovania

07.12.2017 (posledná aktualizácia 27.12.2017)

CVE

CVE-2017-14184

Zasiahnuté systémy

FortiClient for Windows: 5.6.0 nižšie verzie,
FortiClient for Mac OSX: 5.6.0 nižšie verzie,
FortiClient SSLVPN Client for Linux: 4.4.2334 a nižšie verzie.

Následky

Neopravený prístup k informáciám

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých produktov na najnovšiu verziu. V prípade Agent systémov možno interný webový server vypnúť.

Zdroje

https://nvd.nist.gov/vuln/detail/CVE-2017-14184
https://fortiguard.com/psirt/FG-IR-17-214

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

Identifikátor

Foxit Reader Multiple Vulnerabilities

Popis

Produkt Foxit Reader obsahuje viacero zraniteľností, ktoré by vzdialený útočník mohol zneužiť na vykonanie ľubovoľného kódu v kontexte aktuálneho procesu. Útočný vektor vyžaduje interakciu používateľa, ktorý musí navštíviť stránku so škodlivým obsahom alebo otvoriť škodlivý súbor.

V prvej skupine zraniteľností nedochádza pred volaním metód k overovaniu existencie objektov.

V druhej skupine zraniteľností nedochádza k správnej validácii používateľských vstupov.

Dátum prvého zverejnenia varovania

20.12.2017 (posledná aktualizácia 28.12.2017)

CVE

CVE-2017-10957, CVE-2017-10958, CVE-2017-10959, CVE-2017-14818, CVE-2017-14819, CVE-2017-14820, CVE-2017-14821, CVE-2017-14822, CVE-2017-14823, CVE-2017-14824, CVE-2017-14825, CVE-2017-14826, CVE-2017-14827, CVE-2017-14828, CVE-2017-14829, CVE-2017-14830, CVE-2017-14831, CVE-2017-14832, CVE-2017-14833, CVE-2017-14834, CVE-2017-14835, CVE-2017-14836, CVE-2017-14837, CVE-2017-16571, CVE-2017-16572, CVE-2017-16573, CVE-2017-16574, CVE-2017-16575, CVE-2017-16576, CVE-2017-16577, CVE-2017-16578, CVE-2017-16579, CVE-2017-16580, CVE-2017-16581, CVE-2017-16582, CVE-2017-16583, CVE-2017-16584, CVE-2017-16585, CVE-2017-16586, CVE-2017-16587, CVE-2017-16588, CVE-2017-16589

Zasiahnuté systémy

Foxit Reader 8.3.1.21155

Následky

Neoprávnené vykonanie kódu

Odporúčania

Používateľom dotknutého softwaru odporúčame bezodkladne vykonať aktualizáciu.

Zdroje

https://www.foxitsoftware.com/support/security-bulletins.php

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.4**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

IOHIDeous - Unpatched macOS Flaw Allows Code Execution, Root Access

Popis

Bezpečnostná zraniteľnosť v IOHIDFamily, súčasti operačného systému Apple MacOS, umožňuje lokálnemu útočníkovi obísť bezpečnostné prvky System Integrity Protection (SIP) a Apple Mobile File Integrity (AMFI), vykonať škodlivý kód a získať administrátorský prístup ku systému.
K uvedenej zraniteľnosti zatiaľ nie je pridelené CVE číslo.

Dátum prvého zverejnenia varovania

1.1.2018

Zasiahnuté systémy

Apple MacOS

Následky

Eskalácia privilégií, Vykonanie škodlivého kódu

Odporúčania

Administrátorom zasiahnutých produktov odporúčame sledovať webový portál výrobcu softvéru a v prípade vydania aktualizácie túto bezodkladne nainštalovať.

Zdroje

https://siguza.github.io/IOHIDeous/
https://github.com/Siguza/IOHIDeous
http://www.securityweek.com/unpatched-macos-flaw-allows-code-execution-root-access

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.0**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

IBM Tivoli Monitoring Remote Code Execution Vulnerability

Popis

Interný webový server v produkte IBM Tivoli Monitoring obsahuje zraniteľnosť, ktorú by vzdialený útočník mohol zneužiť na vykonanie ľubovoľného kódu alebo spôsobenie pádu aplikácie a následné odopretie služby.

Dátum prvého zverejnenia varovania

13.12.2017 (posledná aktualizácia 27.12.2017)

CVE

CVE-2017-1635

Zasiahnuté systémy

IBM Tivoli Monitoring V6 6.2.2.x

Následky

Neoprávnené vykonanie kódu, Eskalácia privilégií

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/133243
http://www-01.ibm.com/support/docview.wss?uid=swg22010554

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

Identifikátor

Multiple Vulnerabilities in Qt for Android

Popis

Qt for Android obsahuje bezpečnostné zraniteľnosti, ktoré by vzdialený útočník mohol zneužiť na vykonanie príkazov OS alebo modifikáciu environment premenných.

Dátum prvého zverejnenia varovania

15.12.2017 (posledná aktualizácia 28.12.2017)

CVE

CVE-2017-10904, CVE-2017-10905

Zasiahnuté systémy

Qt for Android verzie pred 5.9.0

Následky

Neoprávnené vykonanie príkazov OS

Odporúčania

Používateľom odporúčame bezodkladne vykonať aktualizáciu na najnovšiu verziu.

Zdroje

https://jvn.jp/en/jp/JVN67389262/index.html
https://www.cvedetails.com/cve/CVE-2017-10905/

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

Identifikátor

Wordpres plugins hiding a backdoor

Popis

Pluginy "Duplicate Page And Post", "No Follow All External Links" a "WP No Eternal Links" boli odstránené z oficiálneho repozitára WordPress pluginov. Bezpečnostný audit uvedených pluginov, ktorý vykonali bezpečnostní experti z Wordfence v zdrojových kódoch odhalil backdoor umožňujúci neautorizovaný prístup do administrátorského rozhrania webu. Pluginy sú súčasťou rozsiahlejšieho útoku, ktorého cieľom je injekcia SEO spamu do WordPress stránok využívajúcich uvedené pluginy.
Backdoor v plugine "Duplicate Page And Post" posiela na cloud-wp.org požiadavku obsahujúcu URL, IP adresu a typ prehliadača, na základe ktorých dochádza k injekcii obsahu do stránok bežných používateľov, webových crawlerov alebo administrátorského rozhrania. Tento typ injekcie sa bežne používa ako forma SEO spamu, ktorá vkladaním spätných odkazov znižuje SEO hodnotenie.
Backdoor v plugine "No Follow All External Links" rovnakým postupom kontaktuje cloud.wpserve.org a na základe odoslaných hodnôt vracia obsah. V prípade, že sa o prístup na stránku pokúša webový crawler (napr. Googlebot), dochádza k injekcii spätných odkazov, ktorými možno dosiahnuť zníženie SEO hodnotenia.
Backdoor v plugine "WP No External Links" pracuje na rovnakom princípe, požiadavky posiela na wpconnect.org. V prípade, že sa o prístup pokúša webový crawler, dochádza k injekcii SEO spamu.
Nakoľko je IP adresa domény wpconnect.org totožná s IP adresou domény cloud-wp.org, Wordfence predpokladá, že uvedené pluginy sú súčasťou jedného rozsiahlejšieho útoku.

Dátum prvého zverejnenia varovania

27.12.2017

Zasiahnuté systémy

CMS WordPress

Následky

Backdoor

Odporúčania

Administrátorom odporúčame bezodkladne odinštalovať napadnuté pluginy a vykonať kontrolu, či už nedošlo k injekcii SEO spamu do stránok. Kontrolu možno vykonať skenom na prítomnosť malwaru prostredníctvom služby alebo pluginu Wordfence alebo prostredníctvom online skenovania na https://www.gravityscan.com. V prípade kompromitácie odporúčame urýchlene vykonať obnovu zo zálohy.

Zdroje

https://www.bleepingcomputer.com/news/security/three-more-wordpress-plugins-found-hiding-a-backdoor/
https://www.wordfence.com/blog/2017/12/plugin-backdoor-supply-chain/

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

Identifikátor

Samsung Internet Browser SOP Bypass/UXSS

Popis

Produkt Samsung Internet Browser obsahuje zraniteľnosť, ktorú by útočník mohol zneužiť na obídenie Same Origin Policy a prostredníctvom UXSS útoku získať neoprávnený prístup k citlivým informáciám.
Útočný vektor spočíva v umiestnení IFRAME elementu do XSLT dát v rámci MHTML súboru. Hodnota *document.domain* JavaScript kódu v inej časti MHTML súboru nezodpovedá doméne hostu MHTML súboru, ale hodnote ľubovoľnej URL v rámci obsahu MHTML súboru.

Dátum prvého zverejnenia varovania

20.12.2017 (posledná aktualizácia 29.12.2017)

CVE

CVE-2017-17692, CVE-2017-17859

Zasiahnuté systémy

Samsung Internet Browser 6.2.01.12

Následky

Eskalácia oprávnení, Neoprávnený prístup k citlivým informáciám

Odporúčania

Používateľom odporúčame bezodkladne vykonať aktualizáciu.

Zdroje

https://vuldb.com/fr/?id.111060
https://nvd.nist.gov/vuln/detail/CVE-2017-17692
https://packetstormsecurity.com/files/145510/Samsung-Internet-Browser-SOP-Bypass.html
https://datarift.blogspot.sk/p/samsung-interent-browser-sop-bypass-cve.html
https://securityonline.info/cve-2017-17692-sop-bypass-samsung/

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 6.4**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Synology Chat Multiple Vulnerabilities

Popis

Produkt Synology Chat obsahuje viacero zraniteľností, ktoré by vzdialený autentifikovaný útočník mohol zneužiť na získanie prístupu k intranetovým súborom a na injekciu webových skriptov a HTML kódu.

Link Preview obsahuje zraniteľnosť typu SSRF (server-side request forgery), ktorá autentifikovanému útočníkovi umožňuje prostredníctvom vytvorených URI stiahnuť lokálne súbory v intranetovej sieti.

Slash Command Creator obsahuje zraniteľnosť typu XSS (cross-site scripting), ktorá autentifikovanému útočníkovi umožňuje prostredníctvom parametrov COMMAND, COMMAND INSTRUCTION alebo DESCRIPTION vykonať injekciu webových skriptov alebo HTML kódu.

Dátum prvého zverejnenia varovania

18.12.2017 (posledná aktualizácia 28.12.2017)

CVE

CVE-2017-15886, CVE-2017-15892

Zasiahnuté systémy

Synology Chat verzií pred 2.0.0-1124

Následky

Neoprávnený prístup k informáciám

Odporúčania

Používateľom odporúčame bezodkladne vykonať aktualizáciu na verziu 2.0.0-1124 alebo vyššie verziu.

Zdroje

https://www.synology.com/en-global/support/security/Synology_SA_17_78