SECURITY BULLETIN

Týždeň 20. 09. 2017 – 26. 09. 2017

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.7**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Cisco Small Business Managed Switches Denial of Service Vulnerability

Popis

Zraniteľnosť v systéme Secure Shell (SSH) softvéru Cisco Small Business Managed Switches by mohla umožniť autentifikovanému, vzdialenému útočníkovi spôsobiť opätovné načítanie postihnutého switchu, čo by viedlo k odmietnutiu služby (DoS).
Zraniteľnosť je spôsobená nesprávnym spracovaním SSH pripojení. Útočník by túto chybu zabezpečenia mohol využiť tým, že sa prihlási na postihnutý switch cez protokol SSH a zašle škodlivú SSH správu.

Dátum prvého zverejnenia varovania

20. 09. 2017

CVE

CVE-2017-6720

Cisco Bug ID

CSCvb48377

Zasiahnuté systémy

Cisco Small Business 300 Series Managed Switches
Cisco Small Business 500 Series Stackable Managed Switches
Cisco 350 Series Managed Switches
Cisco 350X Series Stackable Managed Switches
Cisco 550X Series Stackable Managed Switches
Cisco ESW2 Series Advanced Switches

Následky

Neprístupnosť služby

Odporúčania

Spoločnosť CISCO vydala aktualizácie na vyššie uvedené systémy, ktoré riešia túto zraniteľnosť. Odporúčame bezodkladne tieto produkty aktualizovať. Takisto odporúčame povoľovať SSH spojenia len z dôveryhodných IP adries.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170920-sbms

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.3**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Cisco Email Security Appliance Denial of Service Vulnerability

Popis

Zraniteľnosť vo funkcii filtrovania e-mailovej komunikácie softvéru Cisco AsyncOS pre zariadenie Cisco Email Security Appliance môže umožniť neoverenému vzdialenému útočníkovi spôsobiť, že postihnuté zariadenie bude mať nedostatok pamäte a prestane skenovať a premenovávať e-mailové správy. Po vyčerpaní systémovej pamäte môže dôjsť k zrúteniu procesu filtrovania, čo má za následok odmietnutie služby (DoS) na zariadení.
Zraniteľnosť je spôsobená nesprávnym overovaním vstupných príloh e-mailov, ktoré obsahujú poškodené polia. Útočník by túto chybu zabezpečenia mohol zneužiť odoslaním e-mailovej správy s prílohou, ktorá obsahuje poškodené polia prostredníctvom cieleného zariadenia. Keď príslušný softvér filtruje prílohu, proces filtrovania by mohol zlyhať, keď systém vyčerpá pamäť a proces sa reštartuje, čo má za následok stav DoS. Po opätovnom spustení procesu filtrovania softvér obnoví filtrovanie rovnakej prílohy, čo spôsobí zlyhanie a opätovné spustenie procesu filtrovania. Úspešné zneužitie by mohlo dovoliť útočníkovi, aby spôsobil opakované odmietnutie služby.

Dátum prvého zverejnenia varovania

20. 09. 2017

CVE

CVE-2017-12215

Cisco Bug ID

CSCvd29354

Zasiahnuté systémy

Cisco AsyncOS Software for Cisco Email Security Appliances

Následky

Neprístupnosť služby

Odporúčania

Spoločnosť CISCO vydala aktualizácie na vyššie uvedené systémy, ktoré riešia túto zraniteľnosť. Odporúčame bezodkladne tieto produkty aktualizovať.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170920-esa

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

Identifikátor

Cisco Unified Customer Voice Portal Operations Console Privilege Escalation Vulnerability

Popis

Zraniteľnosť funkcie obnovenia prístupov v Operations, Administration, Maintenance, and Provisioning (OAMP) v Cisco Unified Customer Voice Portal (CVP) by mohla umožniť autentifikovanému, vzdialenému útočníkovi získať zvýšené privilégiá.
Zraniteľnosť je spôsobená nesprávnym overením prístupov. Útočník by mohol zneužiť túto chybu zabezpečením autentifikácie na OAMP a odoslaním požadovanej žiadosti HTTP. Úspešný exploit by mohol umožniť útočníkovi získať oprávnenia administrátora. Útočník musí úspešne autentifikovane vstúpiť do systému, aby zneužil túto chybu.

Dátum prvého zverejnenia varovania

20. 09. 2017

CVE

CVE-2017-12214

Cisco Bug ID

CSCve92752

Zasiahnuté systémy

Cisco Unified Customer Voice Portal (CVP) vo verziách 10.5, 11.0 a 11.5

Následky

Neoprávnené zvýšenie privilégií

Odporúčania

Spoločnosť CISCO vydala aktualizácie na vyššie uvedené systémy, ktoré riešia túto zraniteľnosť. Odporúčame bezodkladne tieto produkty aktualizovať.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170920-cvp

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 4.1**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Samba - Server memory information leak over SMB1

Popis

Všetky verzie programu Samba sú ohrozené zraniteľnosťou, ktorá môže viesť k úniku informácií o serverovej pamäti nad SMB1, ak klient môže zapisovať údaje do zdieľania. Niektoré požiadavky na písanie SMB1 neboli správne overené, aby sa zabezpečilo, že klient poslal dostatok údajov na splnenie zápisu, čo umožní zapísať obsah pamäti servera do súboru (alebo tlačiarne) namiesto údajov dodaných klientom. Klient nemôže kontrolovať oblasť pamäte servera, ktorá je zapísaná do súboru (alebo tlačiarne).

Dátum prvého zverejnenia varovania

20. 09. 2017

CVE

CVE-2017-12163

Zasiahnuté systémy

Všetky verzie Samby do verzie 4.6.7

Následky

Únik citlivých informácií

Odporúčania

V dostupných aktualizáciách Samby je táto zraniteľnosť vyriešená. Odporúčame preto bezodkladnú aktualizáciu Samby.

Zdroje

https://www.samba.org/samba/security/CVE-2017-12163.html

SECURITY BULLETIN

Týždeň 20. 09. 2017 – 26. 09. 2017

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

Identifikátor

Samba - SMB3 connections don't keep encryption across DFS redirects

Popis

Nástroje príkazového riadku klienta, ako je 'smbclient', ako aj aplikácie používajúce knižnice 'libsmbclient' vyžadujú šifrovanie. Toto je aktivované v príkazovom riadku pomocou '-e | --encrypt' alebo pomocou knižnice smbc_setOptionSmbEncryptionLevel ().

V predvolenom nastavení sa používa iba SMB1 na pripojenie k serveru, pretože je efektívnym predvoleným nastavením pre možnosť 'client max protocol' smb.conf a '-m | -max-protocol =' a možnosť príkazového riadka je 'NT1 '.

Ak pôvodné pripojenie klienta používa šifrovanie, potom by presmerovanie DFS na iný server malo vynútiť šifrovanie. To je dôležité, pretože tieto presmerovania sú otvorené pre aplikáciu.

V prípade, že boli ako protokol 'max' použité SMB3, SMB3_00, SMB3_02, SMB3_10 alebo SMB3_11 a pripojenie skutočne využíva šifrovanie SMB3, každé presmerované spojenie by stratilo požiadavku na šifrovanie a tiež požiadavky na podpis. To znamená, že útočník by mohol využiť útok man in the middle a mohol by čítať a / alebo meniť obsah spojenia.

Dátum prvého zverejnenia varovania

20. 09. 2017

CVE

CVE-2017-12151

Zasiahnuté systémy

Verzie Samba 4.1.0 do 4.6.7

Následky

Únik citlivých informácií

Odporúčania

V dostupných aktualizáciách Samby je táto zraniteľnosť vyriešená. Odporúčame preto bezodkladnú aktualizáciu Samby.

Zdroje

https://www.samba.org/samba/security/CVE-2017-12151.html

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

Identifikátor

Samba SMB1/2/3 connections may not require signing where they should

Popis

Bolo zistené, že Samba nevyžadovala podpísanie SMB (SMB signing), keď boli povolené určité možnosti konfigurácie. Vzdialený útočník by mohol spustiť útok typu man-in-the-middle a získať informácie v nezašifrovanom texte.

Dátum prvého zverejnenia varovania

20. 09. 2017

CVE

CVE-2017-12150

Zasiahnuté systémy

Verzie Samba 3.0.25 do 4.6.7

Následky

Únik citlivých informácií

Odporúčania

V dostupných aktualizáciách Samby je táto zraniteľnosť vyriešená. Odporúčame preto bezodkladnú aktualizáciu Samby.

Zdroje

https://www.samba.org/samba/security/CVE-2017-12150.html

SECURITY BULLETIN

Týždeň 20. 09. 2017 – 26. 09. 2017

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 4.0**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Joomla! - Core - Information Disclosure

Popis

Logická chyba v dotaze SQL môže viesť k odhaleniu úvodných textov článkov, keď sú tieto články v archivovanom stave.

Dátum prvého zverejnenia varovania

Reportované 04. 08. 2017, opravené 19. 09. 2017

CVE

CVE-2017-14595

Zasiahnuté systémy

Content Management System (CMS) Joomla! vo verziách 3.7.0 až 3.7.5

Následky

Neoprávnený prístup k informáciám

Odporúčania

Odporúčame bezodkladne aktualizovať CMS Joomla! na najnovšiu verziu 3.0.8.

Zdroje

https://developer.joomla.org/security-centre/710-20170901-core-information-disclosure

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 5.7**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Joomla! - Core - LDAP Information Disclosure

Popis

Nedostatočný escaping v LDAP plugine overovania môže mať za následok neoprávnený prístup k používateľskému menu a heslu.

Dátum prvého zverejnenia varovania

Reportované 27. 07. 2017, opravené 19. 09. 2017

CVE

CVE-2017-14596

Zasiahnuté systémy

Content Management System (CMS) Joomla! vo verziách 1.5.0 až 3.7.5

Následky

Neoprávnený prístup k informáciám

Odporúčania

Odporúčame bezodkladne aktualizovať CMS Joomla! na najnovšiu verziu 3.0.8.

Zdroje

https://developer.joomla.org/security-centre/711-20170902-core-ldap-information-disclosure

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

Identifikátor

Chrome Security Updates Relases

Popis

Spoločnosť Google vydala dôležité aktualizácie na produkt Google Chrome, ktorý obsahuje niekoľko opráv zraniteľností s vysokou dôležitosťou.

Dátum prvého zverejnenia varovania

21. 09. 2017

CVE

CVE-2017-5121, CVE-2017-5122

Zasiahnuté systémy

Prehliadač Google Chrome na platformách Linux, Mac a Windows

Následky

Neoprávnený prístup k citlivým informáciám

Odporúčania

Odporúčame bezodkladne aktualizovať prehliadač Google Chrome a následne ho udržovať neustále aktualizovaný.

Zdroje

https://chromereleases.googleblog.com/2017/09/stable-channel-update-for-desktop_21.html

SECURITY BULLETIN

Týždeň 20. 09. 2017 – 26. 09. 2017

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.2**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Security updates for macOS High Sierra 10.13

Popis

Spoločnosť Apple vydala dôležité aktualizácie na produkt macOS High Sierra, ktorý obsahuje niekoľko opráv zraniteľností s vysokou dôležitosťou.
Zároveň v novej verzii 10.13, ktorá obsahuje aj opravu zraniteľností pod CVE uvedenými nižšie, bola objavená ďalšia, doposiaľ nevyriešená zraniteľnosť, ktorá umožňuje útočníkovi s prístupom k nezaheslovanému počítaču odcudziť heslá z Keychain. To je možné cez spustený škodlivý kód alebo spustenú škodlivú aplikáciu. Aplikácie, ktoré sú spustené v systéme, totiž môžu pristupovať ku Keychain bez interakcie používateľa. Útočník pritom môže získať údaje z Keychain v nešifrovanej podobe.

Dátum prvého zverejnenia varovania

25. 09. 2017

CVE

CVE-2017-7084, CVE-2017-7074, CVE-2017-7143, CVE-2017-7083, CVE-2017-0381, CVE-2017-7138, CVE-2017-7121, CVE-2017-7122, CVE-2017-7123, CVE-2017-7124, CVE-2017-7125, CVE-2017-7126, CVE-2017-11103, CVE-2017-7077, CVE-2017-7119, CVE-2017-7114, CVE-2017-7086, CVE-2017-1000373, CVE-2016-9063, CVE-2017-9233, CVE-2017-7141, CVE-2017-7078, CVE-2017-6451, CVE-2017-6452, CVE-2017-6455, CVE-2017-6458, CVE-2017-6459, CVE-2017-6460, CVE-2017-6462, CVE-2017-6463, CVE-2017-6464, CVE-2016-9042, CVE-2017-7082, CVE-2017-7080, CVE-2017-10989, CVE-2017-7128, CVE-2017-7129, CVE-2017-7130, CVE-2017-7127, CVE-2016-9840, CVE-2016-9841, CVE-2016-9842, CVE-2016-9843

Zasiahnuté systémy

macOS High Sierra

Následky

Neoprávnený prístup k citlivým informáciám, Zneprístupnenie služby, Neoprávnené zvýšenie privilégií

Odporúčania

Pri aktualizovaní na macOS High Sierra na verziu 10.13 odporúčame nesťahovať nové aplikácie z internetu až do vydania novej aktualizácie, ktorá vyrieši možnosť úniku hesiel z Keychain.

Zdroje

https://support.apple.com/en-us/HT208144
https://gizmodo.com/high-sierra-reportedly-has-a-password-problem-1818734894

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

Identifikátor

Security updates for iCloud for Windows 7.0

Popis

Spoločnosť Apple vydala dôležité aktualizácie na produkt iCloud pre Windows, ktorý obsahuje niekoľko opráv zraniteľností s vysokou dôležitosťou.

Dátum prvého zverejnenia varovania

25. 09. 2017

CVE

CVE-2017-7127, CVE-2017-7081, CVE-2017-7087, CVE-2017-7091, CVE-2017-7092, CVE-2017-7093, CVE-2017-7094, CVE-2017-7095, CVE-2017-7096, CVE-2017-7098, CVE-2017-7099, CVE-2017-7100, CVE-2017-7102, CVE-2017-7104, CVE-2017-7107, CVE-2017-7111, CVE-2017-7117, CVE-2017-7120, CVE-2017-7089, CVE-2017-7090, CVE-2017-7106, CVE-2017-7109

Zasiahnuté systémy

iCloud pre Windows

Následky

Neoprávnený prístup k citlivým informáciám, Zneprístupnenie služby, Neoprávnené zvýšenie privilégií

Odporúčania

Odporúčame bezodkladne aktualizovať iCloud pre Windows a následne ho udržovať neustále aktualizovaný.

Zdroje

https://support.apple.com/en-us/HT208142

SECURITY BULLETIN

Týždeň 20. 09. 2017 – 26. 09. 2017

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 9.8**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Security updates for macOS Server 5.4

Popis

Spoločnosť Apple vydala dôležité aktualizácie na produkt macOS Server, ktorý obsahuje niekoľko opráv zraniteľností s vysokou dôležitosťou.

Dátum prvého zverejnenia varovania

25. 09. 2017

CVE

CVE-2017-10978, CVE-2017-10979

Zasiahnuté systémy

macOS Server

Následky

Neoprávnený prístup k citlivým informáciám, Zneprístupnenie služby, Neoprávnené zvýšenie privilégií

Odporúčania

Odporúčame bezodkladne aktualizovať macOS Server a následne ho udržovať neustále aktualizovaný.

Zdroje

https://support.apple.com/en-us/HT208102

SECURITY BULLETIN

Týždeň 20. 09. 2017 – 26. 09. 2017

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☐ **Vysoká**	☒ **Kritická**	**CVSS skóre: 9.8**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Oracle – opravy kritických zraniteľností vo viacerých produktoch

Popis

Plugin REST v Apache Struts vo verzii 2.1.2 až 2.3.x pred verziou 2.3.34 a vo verzii 2.5.x pred verziou 2.5.13 používa XStreamHandler s inštanciou XStream na deserializáciu bez akéhokoľvek filtrovania, čo môže viesť k vzdialenému vykonávaniu kódu pri deserializácii XML payloads.

Táto zraniteľnosť môže byť vzdialene exploitovaná bez autentifikácie, teda môže byť zneužitá v sieti bez potreby vyžiadania používateľských prístupov.

Dátum prvého zverejnenia varovania

22. 09. 2017

CVE

CVE-2017-9805

Zasiahnuté systémy

Všetky zasiahnuté produkty nájdete na:
http://www.oracle.com/technetwork/security-advisory/cve-2017-9805-products-3905487.html

Následky

Neoprávnený prístup k citlivým informáciám, neoprávnené vykonanie škodlivého kódu

Odporúčania

Odporúčame bezodkladne aktualizovať produkty Oracle, uvedené v zozname na vyššie uvedenom odkaze.

Zdroje

http://www.oracle.com/technetwork/security-advisory/alert-cve-2017-9805-3889403.html
https://nvd.nist.gov/vuln/detail/CVE-2017-9805

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-008