SECURITY BULLETIN

Týždeň 27. 09. 2017 – 03. 10. 2017

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

Identifikátor

Cisco IOS and IOS XE Software Plug-and-Play PKI API Certificate Validation Vulnerability

Popis

Zraniteľnosť vo webovom grafickom rozhraní (GUI) Wireless LAN Controler softvéru Cisco IOS XE pre Cisco 5760 Wireless LAN Controller, Cisco Catalyst 4500E Supervisor Engine 8-E (Wireless) switche a Cisco New Generation Wireless Controllers (NGWC) 3850 by mohli umožniť autentifikovanému, vzdialenému útočníkovi, aby zvýšil svoje privilégiá na zraniteľnom zariadení.

Zraniteľnosť je spôsobená neúplným overovaním vstupných požiadaviek HTTP zraniteľným grafickým rozhraním, ak sa zmení stav pripojenia GUI alebo protokol. Útočník by túto chybu zabezpečenia mohol využiť tým, že sa autentifikuje na GUI Wireless LAN Controller ako Lobby Administrator a následne zmení stav alebo protokol na pripojenie ku GUI.

Dátum prvého zverejnenia varovania

27. 09. 2017

CVE

CVE-2017-12226

Vendor ID (Cisco Bug ID)

CSCvd73746

Zasiahnuté systémy

Cisco 5760 Wireless LAN Controllers, Cisco Catalyst 4500E Supervisor Engine 8-E (Wireless) Switches, Cisco New Generation Wireless Controllers (NGWC) 3850

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-20170927-ngwc

SECURITY BULLETIN

Týždeň 27. 09. 2017 – 03. 10. 2017

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.7**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Cisco IOS and IOS XE Software Plug-and-Play PKI API Certificate Validation Vulnerability

Popis

Zraniteľnosť aplikácie Cisco IOS Plug and Play a softvéru Cisco IOS XE by mohla umožniť neautentifikovanému vzdialenému útočníkovi získať neoprávnený prístup k citlivým údajom pomocou neplatného certifikátu.
Zraniteľnosť je spôsobená nedostatočným overovaním certifikátu príslušným softvérom. Útočník by túto chybu zabezpečenia mohol zneužiť poskytnutím vytvoreného certifikátu zraniteľnému zariadeniu. Úspešné zneužitie by mohlo umožniť útočníkovi, aby vykonal útoky typu "man-in-the-middle" na dešifrovanie dôverných informácií o pripojeniach používateľov k zraniteľnému softvéru.

Dátum prvého zverejnenia varovania

27. 09. 2017

CVE

CVE-2017-12228

Vendor ID (Cisco Bug ID)

CSCvc33171

Zasiahnuté systémy

Cisco IOS Software a Cisco IOS XE s povolenou aplikáciou Plug-and-Play

Následky

Únik citlivých údajov

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-20170927-pnp

SECURITY BULLETIN

Týždeň 27. 09. 2017 – 03. 10. 2017

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.6**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Cisco IOS Software Network Address Translation Denial of Service Vulnerability

Popis

Zraniteľnosť pri implementácii funkcie Network Address Translation (NAT) v softvéri Cisco IOS by mohla umožniť neautentifikovanému, vzdialenému útočníkovi spôsobiť odmietnutie služby (DoS) na zraniteľnom zariadení.
Táto chyba je spôsobená nesprávnym prekladom H.323 paketov, ktoré používajú protokol Registration, Admission, and Status (RAS) a sú odosielané na postihnuté zariadenie prostredníctvom IPv4. Útočník by túto chybu zabezpečenia mohol zneužiť odoslaním upraveného paketu H.323 RAS na postihnuté zariadenie.

Dátum prvého zverejnenia varovania

27. 09. 2017

CVE

CVE-2017-12231

Vendor ID (Cisco Bug ID)

CSCvc57217

Zasiahnuté systémy

Zariadenia s Cisco IOS Software

Následky

Zneprístupnenie 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-20170927-nat

Dôležitosť	☐ Nízka	☐ Stredná	☒ Vysoká	☐ Kritická	CVSS skóre: 8.6
Klasifikácia	☒ TLP (WHITE)	☐ Vyhradené	☐ Dôverné	☐ Tajné	
Kód sektora (dopad)					

Identifikátor

Cisco IOS Software for Cisco Industrial Ethernet Switches PROFINET Denial of Service Vulnerability

Popis

Zraniteľnosť pri implementácii protokolu PROFINET Discovery and Configuration Protocol (PN-DCP) pre softvér Cisco IOS by mohla umožniť neautentifikovanému vzdialenému útočníkovi spôsobiť reštart zraniteľného zariadenia, čo by malo za následok stav DoS.
Zraniteľnosť je spôsobená nesprávnou analýzou vstupných paketov, ktoré sú zodpovedné za identifikáciu požiadavky PN-DCP a ktoré sú určené pre zraniteľné zariadenie. Útočník by túto chybu zabezpečenia mohol využiť tým, že pošle spracovaný paket žiadosti o identifikáciu PN-DCP na postihnuté zariadenie a potom pokračuje v odosielaní bežných paketov identifikácie žiadosti PN-DCP do zariadenia.

Dátum prvého zverejnenia varovania

27. 09. 2017

CVE

CVE-2017-12235

Vendor ID (Cisco Bug ID)

CSCuz47179

Zasiahnuté systémy

Cisco IOS Software pre Cisco Industrial Ethernet switche

Následky

Zneprístupnenie 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-20170927-profinet

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.6**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Cisco IOS and IOS XE Software Internet Key Exchange Denial of Service Vulnerability

Popis

Zraniteľnosť modulu Internet Key Exchange verzie 2 (IKEv2) softvéru Cisco IOS a softvéru Cisco IOS XE môže umožniť neautentifikovanému vzdialenému útočníkovi spôsobiť vysoké využitie procesora, vzdialené vykonanie kódu alebo reštart postihnutého zariadenia, ktorý vedie k odmietnutiu služby (DoS).
Zraniteľnosť je spôsobená tým, ako postihnuté zariadenie spracováva určité pakety IKEv2. Útočník by túto chybu zabezpečenia môže zneužiť odoslaním špecifických paketov IKEv2 do postihnutého zariadenia.

Dátum prvého zverejnenia varovania

27. 09. 2017

CVE

CVE-2017-12237

Vendor ID (Cisco Bug ID)

CSCvc41277

Zasiahnuté systémy

Cisco IOS Software alebo Cisco IOS XE Software s povolením protokolu Internet Security Association and Key Management Protocol (ISAKMP).

Následky

Zneprístupnenie 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-20170927-ike

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.6**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Cisco IOS Software Common Industrial Protocol Request Denial of Service Vulnerabilities

Popis

Viaceré zraniteľnosti pri implementácii funkcie Common Industrial Protocol (CIP) v softvéri Cisco IOS by mohli umožniť neautentifikovanému vzdialenému útočníkovi spôsobiť reštart zraniteľného zariadenia, čo by viedlo k odmietnutiu služby (DoS).
Zraniteľnosti sú spôsobené nesprávnym analyzovaním vytvorených paketov CIP určených pre postihnuté zariadenie. Útočník by mohol zneužiť tieto zraniteľnosti odoslaním upravených paketov CIP, ktoré majú byť spracované.

Dátum prvého zverejnenia varovania

27. 09. 2017

CVE

CVE-2017-12233, CVE-2017-12234

Vendor ID (Cisco Bug ID)

CSCuz95334, CSCvc43709

Zasiahnuté systémy

Cisco IOS Software alebo Cisco IOS XE Software s povolením Common Industrial Protocol (CIP).

Následky

Zneprístupnenie 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-20170927-cip

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

Identifikátor

Cisco IOS XE Software Locator/ID Separation Protocol Authentication Bypass Vulnerability

Popis

Zraniteľnosť pri implementácii protokolu Locator/ID Separation Protocol (LISP) v softvéri Cisco IOS XE by mohla umožniť neautentifikovanému vzdialenému útočníkovi používať x tunnel router na vynechanie overovacích autentifikácií vykonaných pri registrácii Endpoint Identifier (EID) do Routing Locator (RLOC) v map serveri / map resolveri (MS / MR).
Zraniteľnosť je spôsobená logickou chybou zavedenou regresiou kódu pre príslušný softvér. Útočník by túto chybu zabezpečenia mohol zneužiť odoslaním špecifických platných žiadostí o map registráciu, ktoré MS / MR akceptujú aj v prípade, že autentifikačné kľúče nezodpovedajú príslušnému softvéru.

Dátum prvého zverejnenia varovania

27. 09. 2017

CVE

CVE-2017-12236

Vendor ID (Cisco Bug ID)

CSCvc18008

Zasiahnuté systémy

Zariadenia s Cisco IOS Software

Následky

Neoprávnený prístup do systému

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-20170927-lisp

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.6**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Cisco IOS XE Software for Cisco ASR 1000 Series and cBR-8 Routers Line Card Console Access Vulnerability

Popis

Zraniteľnosť portov na základnej doske Cisco ASR 1000 Series Aggregation Services routerov a Cisco cBR-8 Converged Broadband routerov by mohla umožniť neautentifikovanému fyzickému útočníkovi prístup k operačnému systému príslušného zariadenia.
Zraniteľnosť spočíva v tom, že na základnej doske hore uvedených routerov je k dispozícii port technickej konzoly (engineering console port), ktorý nevyžaduje autentifikáciu. Útočník by túto chybu zabezpečenia mohol využiť fyzicky pripojením k portu konzoly. Úspešný exploit by mohol umožniť útočníkovi získať plný prístup k operačnému systému príslušného zariadenia.

Dátum prvého zverejnenia varovania

27. 09. 2017

CVE

CVE-2017-12239

Vendor ID (Cisco Bug ID)

CSCvc65866, CSCve77132

Zasiahnuté systémy

Cisco ASR 1000 Series Aggregation Services routre a Cisco cBR-8 Converged Broadband Routre

Následky

Neoprávnený prístup do systému

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-20170927-cc

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

Identifikátor

Cisco IOS Software for Cisco Catalyst 6800 Series Switches VPLS Denial of Service Vulnerability

Popis

Zraniteľnosť v zdrojovom kóde služby Virtual Private LAN Service (VPLS) softvéru Cisco IOS pre switche Cisco Catalyst 6800 Series by mohla umožniť neautentifikovanému útočníkovi, aby spôsobil pád karty typu C6800-16P10G alebo C6800-16P10G-XL a tým odmietnutie služby (DoS).
Zraniteľnosť je spôsobená problémom správy pamäte v príslušnom softvéri. Útočník by túto chybu zabezpečenia mohol zneužiť vytvorením veľkého počtu položiek MAC adries generovaných VPLS v tabuľke MAC adries zraniteľného zariadenia.

Dátum prvého zverejnenia varovania

27. 09. 2017

CVE

CVE-2017-12238

Vendor ID (Cisco Bug ID)

CSCva61927

Zasiahnuté systémy

Cisco Catalyst 6800 Series switche

Následky

Zneprístupnenie 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-20170927-vpls

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

Identifikátor

Cisco IOS Software for Cisco Integrated Services Routers Generation 2 Denial of Service Vulnerability

Popis

Zraniteľnosť pri implementácii protokolu v routeroch Cisco IOS 2 (ISR G2) s integrovanými službami (CIS) by mohla umožniť neautentifikovanému útočníkovi spôsobiť reštart zraniteľného zariadenia, čo by viedlo k odmietnutiu služby (DoS).
Zraniteľnosť je dôsledkom nesprávneho klasifikácie rámcov siete Ethernet. Útočník by mohol túto chybu zneužiť odoslaním vytvoreného Ethernet rámca na postihnuté zariadenie.

Dátum prvého zverejnenia varovania

27. 09. 2017

CVE

CVE-2017-12232

Vendor ID (Cisco Bug ID)

CSCvc03809

Zasiahnuté systémy

Cisco IOS Software pre routre Cisco Integrated Services druhej generácie

Následky

Zneprístupnenie 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-20170927-rbip-dos

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

Identifikátor

Cisco IOS XE Wireless Controller Manager Denial of Service Vulnerability

Popis

Zraniteľnosť vo Wireless controller manager softvéru Cisco IOS XE môže umožniť neautentifikovanému útočníkovi spôsobiť reštart switchu a vyústiť do stavu odmietnutia služby (DoS).
Zraniteľnosť je spôsobená nedostatočným overovaním vstupov.

Dátum prvého zverejnenia varovania

27. 09. 2017

CVE

CVE-2017-12222

Vendor ID (Cisco Bug ID)

CSCvd45069

Zasiahnuté systémy

Cisco Catalyst 3650 a 3850 switche, ktoré používajú IOS XE softvér verzie 16.1 do 16.3.3

Následky

Zneprístupnenie 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-20170927-ios-xe

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

Identifikátor

Apache Tomcat Remote Code Execution via JSP Upload Vulnerability

Popis

Pri spustení s povolenými požiadavkami http typu PUT (napríklad nastavením inicializačného parametra readonly na Default servlet na hodnotu false) je možné na server nahrať súbor JSP cez špeciálne vytvorenú požiadavku. Akýkoľvek kód, ktorý by bol obsahom tohto JSP súboru, by bol vykonaný serverom.

Dátum prvého zverejnenia varovania

03. 10. 2017

CVE

CVE-2017-12617

Zasiahnuté systémy

Apache Tomcat od verzie 9.0.0.M1 do 9.0.0
Apache Tomcat od verzie 8.5.0 do 8.5.22
Apache Tomcat od verzie 8.0.0.RC1 do 8.0.46
Apache Tomcat od verzie 7.0.0 do 7.0.81

Následky

Neoprávnené vykonanie škodlivého kódu

Odporúčania

Na vyššie uvedené systémy boli vydané aktualizácie, ktoré riešia túto zraniteľnosť. Odporúčame bezodkladne tieto produkty aktualizovať.

Zdroje

http://mail-archives.us.apache.org/mod_mbox/www-announce/201710.mbox/%3cf7229e11-5e8d-aa00-ff22-f0a795669010@apache.org%3e

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

Identifikátor

Security vulnerabilities fixed in Firefox 56

Popis

Spoločnosť Mozilla vydala dôležité aktualizácie na produkt Firefox 56, ktoré obsahujú niekoľko opráv zraniteľností s vysokou dôležitosťou.

Dátum prvého zverejnenia varovania

28. 09. 2017

CVE

Kompletný zoznam CVE na: https://www.mozilla.org/en-US/security/advisories/mfsa2017-21/

Zasiahnuté systémy

Mozilla Firefox 56

Následky

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

Odporúčania

Odporúčame bezodkladne aktualizovať Mozillu Firefox 56 a následne ho udržovať neustále aktualizovaný.

Zdroje

https://www.mozilla.org/en-US/security/advisories/mfsa2017-21/

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

Identifikátor

Security vulnerabilities fixed in Firefox ESR52.4

Popis

Spoločnosť Mozilla vydala dôležité aktualizácie na produkt Firefox ESR52.4, ktoré obsahujú niekoľko opráv zraniteľností s vysokou dôležitosťou.

Dátum prvého zverejnenia varovania

28. 09. 2017

CVE

Kompletný zoznam CVE na: https://www.mozilla.org/en-US/security/advisories/mfsa2017-22/

Zasiahnuté systémy

Mozilla Firefox ESR52.4

Následky

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

Odporúčania

Odporúčame bezodkladne aktualizovať Mozillu Firefox ESR52.4 a následne ho udržovať neustále aktualizovaný.

Zdroje

https://www.mozilla.org/en-US/security/advisories/mfsa2017-22/

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

Identifikátor

Security updates for iOS 11.0.2

Popis

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

Dátum prvého zverejnenia varovania

26. 09. 2017

CVE

Kompletný zoznam CVE na: https://support.apple.com/sk-sk/HT208112

Zasiahnuté systémy

iOS – mobilné zariadenia iPhone a iPad

Následky

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

Odporúčania

Odporúčame bezodkladne aktualizovať iOS na vašich zariadeniach a následne ho udržovať neustále aktualizovaný.

Zdroje

https://support.apple.com/sk-sk/HT208112