SECURITY BULLETIN

Týždeň 18. 10. 2017 – 24. 10. 2017

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

Identifikátor

Cisco FXOS and NX-OS System Software Authentication, Authorization, and Accounting Denial of Service Vulnerability

Popis

Zraniteľnosť v autentifikácii, autorizácii a zaznamenávanie (authentication, authorization, and accounting - AAA) implementácie systému Cisco Firepower Extensible Operating System (FXOS) a systémového softvéru NX-OS môže umožniť neoverenému vzdialenému útočníkovi spôsobiť reštart dotknutého zariadenia.

Táto chyba sa vyskytuje z dôvodu chyby procesov AAA, ktoré zabraňujú Systémovému správcovi v NX-OS prijímať keepalive správy, keď sa na zariadení vyskytne vysoké množstvo pokusov o prihlásenie, ako napríklad pri brute force útokoch.

Dátum prvého zverejnenia varovania

18. 10. 2017

CVE

CVE-2017-3883

Vendor ID (Cisco Bug ID)

CSCuq58760, CSCuq71257, CSCur97432, CSCus05214, CSCux54898, CSCvc33141, CSCvd36971, CSCve03660

Zasiahnuté systémy

Firepower 4100 Series Next-Generation Firewall, Firepower 9300 Security Appliance, Multilayer Director Switche, Nexus 1000V Series Switche, Nexus 1100 Series Cloud Service Platforms, Nexus 2000 Series Switche, Nexus 3000 Series Switche, Nexus 3500 Platform Switche, Nexus 5000 Series Switche, Nexus 5500 Platform Switche, Nexus 5600 Platform Switche, Nexus 6000 Series Switche, Nexus 7000 Series Switche, Nexus 7700 Series Switche, Nexus 9000 Series Switche v NX-OS móde, Nexus 9500 R-Series Line Cards a Fabric Modules, Unified Computing System (UCS) 6100 Series Fabric Interconnects, UCS 6200 Series Fabric Interconnects, UCS 6300 Series Fabric Interconnects

Následky

Zneprístupnenie služby

Odporúčania

Spoločnosť CISCO vydala aktualizácie na vyššie uvedené produkty, ktoré opravujú jednotlivé zraniteľnosti. Odporúčame bezodkladne tieto produkty aktualizovať.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171018-aaavty

SECURITY BULLETIN

Týždeň 18. 10. 2017 – 24. 10. 2017

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

Identifikátor

Cisco Small Business SPA50x, SPA51x, and SPA52x Series IP Phones SIP Denial of Service Vulnerability

Popis

Zraniteľnosť v implementácii protokolu SIP (Session Initiation Protocol) v IP telefónoch Cisco Small Business série SPA50x, SPA51x a SPA52x môže umožniť neoverenému vzdialenému útočníkovi spôsobiť, zneprístupnenie služby (DoS).
Zraniteľnosť je spôsobená nesprávnym spracovaním správ žiadostí SIP dotknutým zariadením. Útočník by mohol zneužiť túto zraniteľnosť pomocou formátovaných špecifikátorov v SIP payload, ktoré sa posielajú na postihnuté zariadenie.

Dátum prvého zverejnenia varovania

18. 10. 2017

CVE

CVE-2017-12260

Vendor ID (Cisco Bug ID)

CSCvc63986

Zasiahnuté systémy

IP telefóny Cisco Small Business SPA50x, SPA51x, a SPA52x, ktoré fungujú na firmvéri 7.6.2SR1 a starších.

Následky

Zneprístupnenie služby

Odporúčania

Spoločnosť CISCO vydala aktualizácie na vyššie uvedené produkty, ktoré opravujú jednotlivé zraniteľnosti. Odporúčame bezodkladne tieto produkty aktualizovať.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171018-sip1

SECURITY BULLETIN

Týždeň 18. 10. 2017 – 24. 10. 2017

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

Identifikátor

Cisco Small Business SPA51x Series IP Phones SIP Denial of Service Vulnerability

Popis

Zraniteľnosť v implementácii protokolu SIP (Session Initiation Protocol) v IP telefónoch Cisco Small Business série SPA51x môže umožniť neoverenému vzdialenému útočníkovi spôsobiť zneprístupnenie služby (DoS).
Zraniteľnosť je spôsobená nesprávnym spracovaním správ žiadostí SIP dotknutým zariadením. Útočník by túto chybu zabezpečenia mohol zneužiť odoslaním chybných SIP správ postihnutému zariadeniu.

Dátum prvého zverejnenia varovania

18. 10. 2017

CVE

CVE-2017-12259

Vendor ID (Cisco Bug ID)

CSCvc63982

Zasiahnuté systémy

IP telefóny Cisco Small Business SPA51x, ktoré fungujú na firmvéri 7.6.2SR1 a starších.

Následky

Zneprístupnenie služby

Odporúčania

Spoločnosť CISCO vydala aktualizácie na vyššie uvedené produkty, ktoré opravujú jednotlivé zraniteľnosti. Odporúčame bezodkladne tieto produkty aktualizovať.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171018-sip

SECURITY BULLETIN

Týždeň 18. 10. 2017 – 24. 10. 2017

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

Identifikátor

Google Chrome - Stable Channel Update for Desktop

Popis

Spoločnosť Google vydala aktualizáciu na svoj produkt Google Chrome, ktorá obsahuje niekoľko opráv zraniteľností s vysokou dôležitosťou.

Dátum prvého zverejnenia varovania

17. 10. 2017

CVE

CVE-2017-5124, CVE-2017-5125, CVE-2017-5126, CVE-2017-5127, CVE-2017-5128, CVE-2017-5129, CVE-2017-5130, CVE-2017-5131, CVE-2017-5132, CVE-2017-5133, CVE-2017-15386, CVE-2017-15387, CVE-2017-15388, CVE-2017-15389, CVE-2017-15390, CVE-2017-15391, CVE-2017-15392, CVE-2017-15393, CVE-2017-15394, CVE-2017-15395

Zasiahnuté systémy

Google Chrome

Následky

Následky podľa jednotlivých zraniteľností

Odporúčania

Spoločnosť Google vydala aktualizáciu – novú verziu Google Chrome 62.0.3202.62 na vyššie uvedený produkt, ktorá opravuje jednotlivé zraniteľnosti. Odporúčame bezodkladne tento produkt aktualizovať.

Zdroje

https://chromereleases.googleblog.com/2017/10/stable-channel-update-for-desktop.html

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

Identifikátor

Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors – Joint Technical Alert

Popis

FBI (Federal Bureau of Investigation) a DHS (Department of Homeland Security) vydala tzv. spojené technické upozornenie (joint Technical Alert), ktoré poskytuje informácie o pokročilých pretrvávajúcich hrozbách (Advanced Persistent Threat - APT), ktoré sú zamerané na vládne subjekty a organizácie v oblasti energetiky, jadrovej energie, dsitribúcie vody, letectva a kritických výrobných odvetví. Táto správa obsahuje Indicators of Compromise (IOC) a technické detaily o taktike, technikách a postupoch (tactics, techniques, and procedures - TTP), ktoré používajú útočníci v sieťach poškodených obetí.

Zasiahnuté systémy

Sieťové systémy a prevádzkové systémy subjektov a organizácií v oblasti energetiky, distribúcie vody, jadrovej energie, letectva a kritických výrobných odvetví

IOC (Indicators of Compromise)

Kompletný list IOC nájdete na tomto odkaze:
https://www.us-cert.gov/sites/default/files/publications/TA17-293A_TLP_WHITE_CSV.csv

MAR (Malware analysis report)

Kompletný MAR nájdete na týchto odkazoch:
https://www.us-cert.gov/sites/default/files/publications/MIFR-10127623_TLP_WHITE.pdf
https://www.us-cert.gov/sites/default/files/publications/MIFR-10128327_TLP_WHITE.pdf
https://www.us-cert.gov/sites/default/files/publications/MIFR-10128336_TLP_WHITE.pdf
https://www.us-cert.gov/sites/default/files/publications/MIFR-10128830_TLP_WHITE.pdf
https://www.us-cert.gov/sites/default/files/publications/MIFR-10128883_TLP_WHITE.pdf
https://www.us-cert.gov/sites/default/files/publications/MIFR-10135300_TLP_WHITE.pdf

Technická analýza

Spoločným menovateľom pre všetky útoky boli fázy zahŕňajúce prieskum, tvorbu škodlivého kódu, rozposlanie, zneužitie zraniteľností, inštaláciu, command and control a útoky na objekty. Kompletnú technickú analýzu nájdete na tomto odkaze:
https://www.us-cert.gov/ncas/alerts/TA17-293A

Sieťové signatúry

Kompletný zoznam sieťových signatúr nájdete na:
https://www.us-cert.gov/ncas/alerts/TA17-293A

HBR (Host-Based Rules)
Kompletný výpis HBR (v tomto prípade YARA) pravidiel nájdete na tomto odkaze: https://www.us-cert.gov/ncas/alerts/TA17-293A

Následky
Viacero možných následkov podľa typu útoku (Zneprístupnenie služby, neoprávnený prístup do systému, Neoprávnený prístup k citlivým informáciám)

Detekcia
Odporúčame administrátorom siete, aby skontrolovali IP adresy, hash súbory, sieťové podpisy a YARA pravidlá a pridali IP adresy, uvedené v IOC súbore vyššie, do svojho monitorovacieho zoznamu, aby zistili, či bola v ich organizácii pozorovaná škodlivá aktivita. Pri kontrole sieťových protokolov a logov z perimetrov siete môžu administrátori nájsť početné prípady podozrivých IP adries, ktoré sa pokúšajú pripojiť k určitým systémom. Pri kontrole komunikácie z týchto IP adries správcovia systému môžu zistiť, že určité prenosy zodpovedajú škodlivým aktivitám a niektorým legitímnym aktivitám. Správcom systémov sa tiež odporúča, aby spustili nástroj YARA na akomkoľvek systéme, o ktorom majú podozrenie, že boli predmetom útoku v rámci tejto kampane.

Odporúčania
Administrátorom siete sa odporúča: - Zabráňte externej komunikácii všetkých verzií SMB protokolu a súvisiacich protokolov na hranici siete blokovaním portov TCP 139 a 445 a UDP 137. - Zablokujte protokol WebDAV na gateway zariadeniach v sieti. - Monitorujte logy kvôli netradičným, abnormálnym aktivitám – napríklad prihlásenia z neoverenej IP adresy, prihlásenia v čase mimo pracovných hodín a pod. - Nasaďte webové a e-mailové filtre vo svojej sieti - Oddeľte kritické prevádzkové a riadiace systémy od ostatných systémov vo vašej sieti - Zabezpečte riadne zaznamenávanie prevádzky na vstupe a výstupe vo vašej sieti

Zdroje
https://www.us-cert.gov/ncas/alerts/TA17-293A