NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

SECURITY BULLETIN

Týždeň 16. 08. 2017 – 22. 08. 2017

No: B20170822-01V

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

Identifikátor

Symantec Messaging Gateway Remote Code Execution

Popis

V Symantec Messaging Gateway môže dôjsť k možnosti vzdialeného spustenia škodlivého kódu, keď útočník môže získať schopnosť vykonať príkazy vzdialene na cieľovom zariadení alebo v cieľovom procese. V tomto type zraniteľnosti sa po získaní prístupu k systému môže útočník pokúsiť zvýšiť svoje privilégiá.

CVE

CVE-2017-6327

Zasiahnuté systémy

Symantec Messaging Gateway do verzie 10.6.3.-267

Následky

Neoprávnené vykonanie škodlivého kódu

Odporúčania

Spoločnosť Symantec vydala bezplatné aktualizácie softvéru, ktoré riešia predmetnú zraniteľnosť. Oprava zraniteľnosti sa nachádza vo verzii 10.6.3.-267. Ak využívate tento produkt, bezodkladne aktualizujte svoje zariadenie.

Zdroje

https://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20170810_00

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-001

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

SECURITY BULLETIN

Týždeň 16. 08. 2017 – 22. 08. 2017

No: B20170822-02V

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

Identifikátor

Symantec Messaging Gateway Cross Site Request Forgery

Popis

Symantec Messaging Gateway obsahuje zraniteľnosť, ktorá je založená na falšovaní žiadostí o cross site request (známy aj ako one-click attack - skrátene ako CSRF alebo XSRF), čo je typ škodlivého zneužívania webovej lokality, kde sú neoprávnené príkazy prenesené od používateľa. Útok CSRF sa pokúša využívať dôveru, ktorú má konkrétny web v prehliadači používateľa.

CVE

CVE-2017-6328

Zasiahnuté systémy

Symantec Messaging Gateway do verzie 10.6.3.-267

Následky

Neoprávnené zvýšenie privilégií

Odporúčania

Spoločnosť Symantec vydala bezplatné aktualizácie softvéru, ktoré riešia predmetnú zraniteľnosť. Oprava zraniteľnosti sa nachádza vo verzii 10.6.3.-267. Ak využívate tento produkt, bezodkladne aktualizujte svoje zariadenie.

Zdroje

https://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20170810_00

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-001

SECURITY BULLETIN

Týždeň 16. 08. 2017 – 22. 08. 2017

No: B20170822-03V

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

Identifikátor

Cisco Application Policy Infrastructure Controller SSH Privilege Escalation Vulnerability

Popis

Zraniteľnosť v APIC (Cisco Application Policy Infrastructure Controller) by mohla umožniť autentifikovanému, vzdialenému útočníkovi získať vyššie oprávnenia než sú priradené k účtu. Útočník dostane privilégiá posledného užívateľa na prihlásenie bez ohľadu na to, či sú tieto privilégiá vyššie alebo nižšie, ako mali byť udelené. Útočník však nemôže získať oprávnenia na úrovni root.

Zraniteľnosť je spôsobená obmedzením toho, ako Role Access Control (RBAC) udeľuje privilégiá vzdialene autentifikovaným používateľom pri prihlasovaní cez SSH priamo do lokálneho rozhrania manažmentu APIC. Útočník by túto chybu zabezpečenia mohol zneužiť overovaním na cielené zariadenie. Úroveň privilégií útočníka bude upravená tak, aby zodpovedala úrovni posledného používateľa na prihlásenie cez SSH.

CVE

CVE-2017-6767

Cisco bug ID

CSCvc34335

Zasiahnuté systémy

Cisco APIC

Následky

Neoprávnené zvýšenie privilégií

Odporúčania

Spoločnosť Cisco vydala bezplatné aktualizácie softvéru, ktoré riešia predmetnú zraniteľnosť. Ak využívate tento produkt, bezodkladne aktualizujte svoje zariadenie.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170816-apic1

SECURITY BULLETIN

Týždeň 16. 08. 2017 – 22. 08. 2017

No: B20170822-04V

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

Identifikátor

Cisco Application Policy Infrastructure Controller Custom Binary Privilege Escalation Vulnerability

Popis

Zraniteľnosť v procese zostavovania určitých spustiteľných systémových súborov nainštalovaných pri zavádzaní na zariadeniach APIC (API) Cisco Application Policy Infrastructure Policy by mohla umožniť autentifikovanému lokálnemu útočníkovi získať oprávnenia na úrovni root.

Táto chyba je spôsobená vlastným spustiteľným súborom, ktorý bol vytvorený pre použitie relatívnych vyhľadávacích ciest pre knižnice bez správneho overenia knižnice na načítanie. Útočník by túto chybu zabezpečenia mohol zneužiť autentifikáciou zariadenia a načítavaním škodlivej knižnice, ktorá môže zvýšiť úroveň privilégií. Úspešný exploit by mohol umožniť útočníkovi získať oprávnenia na úrovni root a prevziať plnú kontrolu nad zariadením. Útočník musí mať platné poverenia používateľa na prihlásenie do zariadenia.

CVE

CVE-2017-6768

Cisco bug ID

CSCvc96087

Zasiahnuté systémy

Cisco APIC

Následky

Neoprávnené zvýšenie privilégií

Odporúčania

Spoločnosť Cisco vydala bezplatné aktualizácie softvéru, ktoré riešia predmetnú zraniteľnosť. Ak využívate tento produkt, bezodkladne aktualizujte svoje zariadenie.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170816-apic2

SECURITY BULLETIN

Týždeň 16. 08. 2017 – 22. 08. 2017

No: B20170822-05V

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

Identifikátor

Cisco Virtual Network Function Element Manager Arbitrary Command Execution Vulnerability

Popis

Zraniteľnosť v Cisco Virtual Network Function (VNF) Element Manager by mohla umožniť autentifikovanému, vzdialenému útočníkovi zvýšiť privilégiá a spustiť príkazy v postavení užívateľa root na serveri.
Táto chyba je spôsobená nastaveniami príkazov, ktoré umožňujú používateľom Cisco VNF Element Manager špecifikovať ľubovoľné príkazy, ktoré budú na serveri pracovať ako root.

CVE

CVE-2017-6710

Cisco bug ID

CSCvc76670

Zasiahnuté systémy

Cisco VNF Element Manager Releases do verzie 5.0.4 a 5.1.4.

Následky

Neoprávnené zvýšenie privilégií, neoprávnené vykonanie škodlivého kódu

Odporúčania

Spoločnosť Cisco vydala bezplatné aktualizácie softvéru, ktoré riešia predmetnú zraniteľnosť. Ak využívate tento produkt, bezodkladne aktualizujte svoje zariadenie.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170816-em

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-001

SECURITY BULLETIN

Týždeň 16. 08. 2017 – 22. 08. 2017

No: B20170822-06V

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

Identifikátor

Mozilla Thunderbird 52.3 important updates

Popis

Spoločnosť Mozilla vydala dôležité aktualizácie na produkt Thunderbird 52.3, ktoré riešia niektoré závažné zraniteľnosti.

CVE

CVE-2017-7800, CVE-2017-7801, CVE-2017-7809, CVE-2017-7784, CVE-2017-7802, CVE-2017-7785, CVE-2017-7786, CVE-2017-7753, CVE-2017-7787, CVE-2017-7807, CVE-2017-7792, CVE-2017-7804, CVE-2017-7791, CVE-2017-7782, CVE-2017-7803, CVE-2017-7779

Zasiahnuté systémy

Thunderbird 52.3

Následky

Neoprávnené spustenie škodlivého kódu, Zneprístupnenie služby, Únik informácií

Odporúčania

Spoločnosť Mozilla vydala komplexnú aktualizáciu vyššie uvedeného produktu, preto odporúčame bezodkladne tento produkt aktualizovať.

Zdroje

https://www.mozilla.org/en-US/security/advisories/mfsa2017-20/

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

SECURITY BULLETIN

Týždeň 16. 08. 2017 – 22. 08. 2017

No: B20170822-07V

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

Identifikátor

DNSSEC Key Signing Key Rollover

Popis

Dňa 11. októbra 2017 Internet Corporation for Assigned Names and Numbers (ICANN) zmení root kľúč na podpisovanie kľúčov (Root Zone Key Signing Key - KSK) používaný v DNS protokole DNSSEC (DNS Security Extensions).

DNSSEC je súbor rozšírení protokolu DNS, ktoré sú používané na digitálne podpísanie informácií o DNS, čo je dôležitá súčasť ochrany názvov domén pred neoprávneným použitím alebo zneužitím. Aktualizácia DNSSEC KSK je dôležitý bezpečnostný krok, podobný aktualizácii koreňového certifikátu PKI. Udržanie aktuálneho Root KSK ako dôveryhodného kľúča je nevyhnutné pre zabezpečenie toho, aby overovanie DNS resolverov aj naďalej fungovalo po zmene root kľúča. Zatiaľ čo validácia DNSSEC je pre štátne inštitúcie, ktoré validáciu DNSSEC používajú, povinná, nevyžaduje sa od súkromného sektora. Systémy organizácií, ktoré nepoužívajú validáciu DNSSEC, nebudú zmenou ovplyvnené zmenou.

KSK root bol už zverejnený, aby sa zabezpečila distribúcia v dostatočnom predstihu.

Zasiahnuté systémy

DNSSEC Key Signing Key

Odporúčania

Ak používate DNSSEC protokol, existujú dve možnosti:

1. Konfigurácia automatickej zmeny root kľúča - väčšina implementácií DNS podporuje automatický protokol zmeny kľúčov špecifikovaný v RFC 5011. Tento protokol umožňuje klientovi DNSSEC automaticky aktualizovať dôveryhodné kľúče, keď dôveryhodná zóna DNS signalizuje, že mení kľúč. Spôsob vykonávania tejto konfigurácie je špecifický pre jednotlivé implementácie, takže správcovia by mali zvážiť tieto kroky v súvislosti s bezpečnostnými pravidlami, ktoré v štruktúre systému platia.
2. Manuálna zmena root kľúča - Ak klient DNS používa protokol DNSSEC, ale nepodporuje protokol automatickej zmeny kľúčov, správcovia musia kľúč aktualizovať ručne. Nový root kľúč môže byť kedykoľvek pridaný k súboru dôveryhodných kľúčov, ale mal by byť pridaný pred zrušením starého kľúča, aby sa zabezpečila kontinuálna prevádzka. Nakoľko zmena kľúčov je naplánovaná na 11. októbra 2017, musí byť root kľúč (ktorý už bol zverejnený) v koreňovej zóne pridaný do 11. októbra 2017.

Zdroje

https://rollready.dnsops.gov/
https://www.icann.org/resources/pages/ksk-rollover

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-001