SECURITY BULLETIN

Týždeň 04. 10. 2017 – 10. 10. 2017

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

Identifikátor

Cisco Adaptive Security Appliance Software Direct Authentication Denial of Service Vulnerability

Popis

Zraniteľnosť v implementácii funkcie priamej autentifikácie v softvéri Cisco Adaptive Security Appliance (ASA) by mohla umožniť neoverenému vzdialenému útočníkovi spôsobiť neočakávaný reštart postihnutého zariadenia, čo by malo za následok stav DoS (DoS).
Zraniteľnosť je spôsobená neúplným overovaním vstupov hlavičky HTTP. Útočník by túto chybu zabezpečenia mohol využiť tým, že pošle spracovanú žiadosť HTTP na lokálnu IP adresu postihnutého zariadenia.

Dátum prvého zverejnenia varovania

04. 10. 2017

CVE

CVE-2017-12246

Vendor ID (Cisco Bug ID)

CSCvd59063

Zasiahnuté systémy

ASA 5500 Series Adaptive Security Appliances; ASA 5500-X Series Next-Generation Firewalls; ASA Services Module for Cisco Catalyst 6500 Series Switche a Cisco 7600 Series Routre; ASA 1000V Cloud Firewall; Adaptive Security Virtual Appliance (ASAv); Firepower 4110 Security Appliance; Firepower 9300 ASA Security Module; ISA 3000 Industrial Security Appliance

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-20171004-asa

SECURITY BULLETIN

Týždeň 04. 10. 2017 – 10. 10. 2017

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

Identifikátor

Cisco Firepower Detection Engine IPv6 Denial of Service Vulnerability

Popis

Zraniteľnosť pri analyzovaní paketov protokolu IPv6 v detection engine softvéru Cisco Firepower System Software môže umožniť neoverenému vzdialenému útočníkovi spôsobiť vysoké využitie procesora alebo spôsobiť stav DoS, pretože sa reštartuje Snort.
Táto chyba je dôsledkom nesprávneho overenia polí v hlavičke IPv6 paketu. Útočník by túto chybu zabezpečenia mohol zneužiť odoslaním škodlivého paketu IPv6 na detection engine na cieľovom zariadení.

Dátum prvého zverejnenia varovania

04. 10. 2017

CVE

CVE-2017-12244

Vendor ID (Cisco Bug ID)

CSCvd34776

Zasiahnuté systémy

3000 Series Industrial Security Appliances (ISR); Adaptive Security Appliance (ASA) 5500-X Series with FirePOWER Services; Adaptive Security Appliance (ASA) 5500-X Series Next-Generation Firewalls; Advanced Malware Protection (AMP) for Networks; 7000 Series Appliances; Advanced Malware Protection (AMP) for Networks, 8000 Series Appliances; FirePOWER 7000 Series Appliances; FirePOWER 8000 Series Appliances; Firepower Threat Defense for Integrated Services Routers (ISRs); Firepower 2100 Series Security Appliances; Firepower 4100 Series Security Appliances; Firepower 9300 Series Security Appliances; Virtual Next-Generation Intrusion Prevention System (NGIPSv) for VMware

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-20171004-fpsnort

SECURITY BULLETIN

Týždeň 04. 10. 2017 – 10. 10. 2017

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

Identifikátor

Cisco Firepower Detection Engine SSL Decryption Memory Consumption Denial of Service Vulnerability

Popis

Zraniteľnosť v dešifrovaní SSL komunikácie v softvéri Cisco Firepower Threat Defense (FTD) by mohla umožniť neoverenému vzdialenému útočníkovi minutie systémovej pamäte. Ak táto strata pamäte pretrváva v priebehu času, mohlo by dôjsť k vytvoreniu podmienok pre odmietnutie poskytovania služby (DoS), pretože prenos môže prestať byť smerovaný cez zariadenie.

Zraniteľnosť je spôsobená chybou v spôsobe, akým Firepower Detection Snort Engine spracováva dešifrovanie a upozornenia na prenos SSL a od zariadenia Adaptive Security Appliance (ASA).

Dátum prvého zverejnenia varovania

04. 10. 2017

CVE

CVE-2017-12245

Vendor ID (Cisco Bug ID)

CSCve02069

Zasiahnuté systémy

Adaptive Security Appliance (ASA) 5500-X Series Next-Generation Firewalls; Firepower 2100 Series Security Appliances; Firepower 4100 Series Security Appliances; Firepower 9300 Series Security Appliances

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-20171004-ftd

SECURITY BULLETIN

Týždeň 04. 10. 2017 – 10. 10. 2017

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 4.4**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

macOS High Sierra 10.13 Supplemental Update

Popis

Spoločnosť Apple vydala na macOS High Sierra 10.13 aktualizáciu, ktorá rieši dve zraniteľnosti:

CVE-2017-7149: Ak bol v nástroji Disk Utility nastavený hint pri vytváraní začiarkavacieho zväzku APFS, heslo bolo uložené ako nápoveda. Útočník tak mohol na lokálnej úrovni získať prístup k šifrovanému zväzku APFS.

CVE-2017-7150: Zraniteľnosť umožňovala 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

05. 10. 2017

CVE

CVE-2017-7149, CVE-2017-7150

Zasiahnuté systémy

macOS High Sierra

Následky

Zneprístupnenie služby

Odporúčania

Spoločnosť Apple vydala aktualizáciu na vyššie uvedený produkt (verziu macOS High Sierra 10.13), ktorý rieši uvedené zraniteľnosti. Odporúčame bezodkladne tieto produkty aktualizovať.

Zdroje

https://support.apple.com/en-us/HT208165