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

Identifikátor

Cisco Firepower 4100 Series NGFW and Firepower 9300 Security Appliance Smart Licensing Command Injection Vulnerability

Popis

Zraniteľnosť v službe Smart Licensing Manager firewallu Cisco Firepower 4100 Series Next-Generation (NGFW) a Firepower 9300 Security Appliance by mohla umožniť autentifikovanému vzdialenému útočníkovi vykonať ľubovoľné príkazy s oprávneniami používateľa root.
Zraniteľnosť je spôsobená nedostatočným overovaním vstupov niektorých konfiguračných parametrov aplikácie Smart Licensing. Autentifikovaný útočník by túto chybu zabezpečenia mohol zneužiť konfiguráciou škodlivej URL adresy v rámci príslušnej funkcie.

Dátum prvého zverejnenia varovania

01. 11. 2017

CVE

CVE-2017-12277

Vendor ID (Cisco Bug ID)

CSCvb86863

Zasiahnuté systémy

Firepower 4100 Series Next-Generation Firewall a Firepower 9300 Security Appliance

Následky

Neoprávnené vykonanie kódu

Odporúčania

Spoločnosť Cisco vydala aktualizáciu na uvedený produkt, ktorá opravuje predmetnú zraniteľnosť. Odporúčame bezodkladne daný produkt aktualizovať.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-fpwr

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

Identifikátor

Cisco Application Policy Infrastructure Controller Enterprise Module Unauthorized Access Vulnerability

Popis

Zraniteľnosť v konfigurácii firewallu produktu môže umožniť neoverenému lokálnemu útočníkovi získať privilegovaný prístup k službám dostupným iba v internej sieti zariadenia. Zraniteľnosť je spôsobená nesprávnym pravidlom firewallu v zariadení. Nesprávna konfigurácia by mohla umožniť preposielanie trafficu na verejné rozhranie zariadenia do internej virtuálnej siete APIC-EM.

Dátum prvého zverejnenia varovania

01. 11. 2017

CVE

CVE-2017-12262

Vendor ID (Cisco Bug ID)

CSCve89638

Zasiahnuté systémy

Cisco Application Policy Infrastructure Controller Enterprise Module do verzie 1.5

Následky

Neoprávnený prístup do systému, neoprávnený prístup k informáciám

Odporúčania

Spoločnosť Cisco vydala aktualizáciu na uvedený produkt, ktorá opravuje predmetnú zraniteľnosť. Odporúčame bezodkladne daný produkt aktualizovať.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-apicem

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

Identifikátor

Cisco Prime Collaboration Provisioning Authenticated SQL Injection Vulnerability

Popis

Zraniteľnosť v kóde webového rámca pre rozhranie SQL databázy aplikácie Cisco Prime Collaboration Provisioning by mohla umožniť autentifikovanému vzdialenému útočníkovi ovplyvniť dôvernosť a integritu aplikácie vykonaním ľubovoľných dotazov SQL. Útočník by mohol čítať alebo zapisovať informácie z/do databázy SQL.
Zraniteľnosť je spôsobená nesprávnym overovaním vstupov dodaných používateľmi v rámci dotazov SQL. Útočník by túto chybu zabezpečenia mohol zneužiť odoslaním upravených adries URL, ktoré obsahujú škodlivé príkazy SQL príslušnej aplikácii. Zneužitie tejto zraniteľnosti by mohlo umožniť útočníkovi zadať určité hodnoty a zapísať škodlivý vstup do databázy SQL. Útočník by potreboval mať platné poverenia používateľa.

Dátum prvého zverejnenia varovania

01. 11. 2017

CVE

CVE-2017-12276

Vendor ID (Cisco Bug ID)

CSCvf47935

Zasiahnuté systémy

Cisco Prime Collaboration Provisioning Software do verzie 12.3

Následky

Neoprávnené vykonanie kódu

Odporúčania

Spoločnosť Cisco vydala aktualizáciu na uvedený produkt, ktorá opravuje predmetnú zraniteľnosť. Odporúčame bezodkladne daný produkt aktualizovať.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-cpcp

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

Identifikátor

Security updates for Google Chrome

Popis

Spoločnosť Google vydala dôležitú aktualizáciu na produkt Google Chrome, ktorá obsahuje niekoľko opráv dôležitých zraniteľností.

Dátum prvého zverejnenia varovania

06. 11. 2017

CVE

CVE-2017-15398, CVE-2017-15399

Zasiahnuté systémy

Google Chrome

Následky

Neoprávnené vykonanie škodlivého kódu

Odporúčania

Odporúčame bezodkladne aktualizovať Google Chrome na verziu 62.0.3202.89 na vašich zariadeniach a následne ho udržovať neustále aktualizovaný.

Zdroje

https://chromereleases.googleblog.com/search/label/Stable%20updates

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

Identifikátor

Cisco Identity Services Engine Privilege Escalation Vulnerability

Popis

Zraniteľnosť v restricted shell služby Cisco Identity Services Engine (ISE), ktorá je prístupná cez SSH, môže umožniť autentifikovanému lokálnemu útočníkovi spustiť ľubovoľné CLI príkazy so zvýšeným oprávnením.
Zraniteľnosť je spôsobená neúplným overovaním užívateľských vstupov pre CLI príkazy vydané v restricted shell. Útočník by mohol zneužiť túto chybu autentifikáciou na cielené zariadenie a vykonaním príkazov, ktoré by mohli viesť k zvýšeniu privilégií.

Dátum prvého zverejnenia varovania

01. 11. 2017

CVE

CVE-2017-12261

Vendor ID (Cisco Bug ID)

CSCve74916

Zasiahnuté systémy

Cisco ISE, Cisco ISE Express a Cisco ISE Virtual Appliance bežiace na Cisco Identity Services Engine verzie 1.4, 2.0, 2.0.1 a 2.1.0

Následky

Neoprávnené zvýšenie privilégií

Odporúčania

Spoločnosť Cisco vydala aktualizáciu na uvedený produkt, ktorá opravuje predmetnú zraniteľnosť. Odporúčame bezodkladne daný produkt aktualizovať.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-ise

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

Identifikátor

Cisco Wireless LAN Controller Simple Network Management Protocol Memory Leak Denial of Service Vulnerability

Popis

Zraniteľnosť v subsystéme Simple Network Management Protocol (SNMP) produktov Cisco Wireless LAN Controllers by mohla umožniť autentifikovanému vzdialenému útočníkovi spôsobiť reštartovanie postihnutého zariadenia, čo by viedlo k odmietnutiu služby (DoS).
Zraniteľnosť je spôsobená únikom pamäte, ku ktorému dochádza na postihnutom zariadení po tom, ako zariadenie nedokáže odstrániť vyrovnávaciu pamäť, ktorá sa používa pri vyhľadávaní niektorých MIB. Útočník, ktorý pozná Read string SNMP verzie 2 alebo má platné poverenia protokolu SNMP verzie 3 pre postihnuté zariadenie, by mohol opakovane vyhľadávať príslušné identifikátory objektov MIB a spotrebúvať dostupnú pamäť v zariadení. Keď je pamäť na zariadení dostatočne vyčerpaná, zariadenie sa reštartuje a výsledkom je stav DoS.

Dátum prvého zverejnenia varovania

01. 11. 2017

CVE

CVE-2017-12278

Vendor ID (Cisco Bug ID)

CSCvc71674

Zasiahnuté systémy

Cisco Wireless LAN Controllers s povoleným Simple Network Management Protocol

Následky

Neprístupnosť služby

Odporúčania

Spoločnosť Cisco vydala aktualizáciu na uvedený produkt, ktorá opravuje predmetnú zraniteľnosť. Odporúčame bezodkladne daný produkt aktualizovať.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-wlc1

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

Identifikátor

Cisco Wireless LAN Controller 802.11v Basic Service Set Transition Management Denial of Service Vulnerability

Popis

Zraniteľnosť v implementácii funkcie 802.11v Basic Service Set (BSS) Transition Management v Cisco Wireless LAN Controllers by mohla umožniť neoverenému priľahlému útočníkovi spôsobiť neočakávaný reštart postihnutého zariadenia, čo má za následok stav neprístupnosti služby (DoS).

Táto zraniteľnosť je spôsobená nedostatočným overovaním vstupov paketov 802.11v BSS Transition Management Response, ktoré postihnuté zariadenie prijíma od bezdrôtových klientov. Útočník by túto chybu zabezpečenia mohol zneužiť odoslaním chybného paketu 802.11v BSS Transition Management Response na postihnuté zariadenie.

Dátum prvého zverejnenia varovania

01. 11. 2017

CVE

CVE-2017-12275

Vendor ID (Cisco Bug ID)

CSCvb57803

Zasiahnuté systémy

Cisco Wireless LAN Controllers

Následky

Neprístupnosť služby

Odporúčania

Spoločnosť Cisco vydala aktualizáciu na uvedený produkt, ktorá opravuje predmetnú zraniteľnosť. Odporúčame bezodkladne daný produkt aktualizovať.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-wlc2

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

Identifikátor

Cisco Aironet 1560, 2800, and 3800 Series Access Point Platforms Extensible Authentication Protocol Denial of Service Vulnerability

Popis

Zraniteľnosť v Extensible Authentication Protocol (EAP), ktorý procesuje vstupné rámce pre Cisco Aironet 1560, 2800, a 3800 Series prístupové body by mohla umožniť neoverenému útočníkovi v dosahu Wi-Fi v rádiovej frekvencii (RF) vrstvy 2 spôsobiť reštart prístupového bodu čo má za následok stav neprístupnosti služby (DoS).
Zraniteľnosť je spôsobená nedostatočným overením EAP rámca. Útočník by túto chybu zabezpečenia mohol zneužiť odoslaním chybného EAP rámca do cieleného zariadenia. V prípade obnovy zariadenia možno bude potrebné manuálne odpojiť a následne zapojiť zariadenie do siete, aby sa reštartlo.

Dátum prvého zverejnenia varovania

Prvé zverejnenie dňa 01. 11. 2017; aktualizácia dňa 02. 11. 2017

CVE

CVE-2017-12274

Vendor ID (Cisco Bug ID)

CSCve18935

Zasiahnuté systémy

Aironet 1560 Series Access Points, Aironet 2800 Series Access Points, Aironet 3800 Series Access Points

Následky

Neprístupnosť služby

Odporúčania

Spoločnosť Cisco vydala aktualizáciu na uvedený produkt, ktorá opravuje predmetnú zraniteľnosť. Odporúčame bezodkladne daný produkt aktualizovať.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-aironet2

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

Identifikátor

Cisco Aironet 1560, 2800, and 3800 Series Access Point Platforms 802.11 Denial of Service Vulnerability

Popis

Zraniteľnosť v protokole 802.11, ktorý procesuje vstupné rámce pre Cisco Aironet 1560, 2800, a 3800 Series prístupové body by mohla umožniť neoverenému útočníkovi v dosahu Wi-Fi v rádiovej frekvencii (RF) vrstvy 2 spôsobiť reštart prístupového bodu čo má za následok stav neprístupnosti služby (DoS).
Zraniteľnosť je spôsobená nedostatočným overením požiadavky protokolu 802.11. Útočník by túto chybu zabezpečenia mohol zneužiť odoslaním škodlivej žiadosti protokolu 802.11 do cieleného zariadenia.

Dátum prvého zverejnenia varovania

Prvé zverejnenie dňa 01. 11. 2017; aktualizácia dňa 02. 11. 2017

CVE

CVE-2017-12273

Vendor ID (Cisco Bug ID)

CSCve12189

Zasiahnuté systémy

Aironet 1560 Series Access Points, Aironet 2800 Series Access Points, Aironet 3800 Series Access Points

Následky

Neprístupnosť služby

Odporúčania

Spoločnosť Cisco vydala aktualizáciu na uvedený produkt, ktorá opravuje predmetnú zraniteľnosť. Odporúčame bezodkladne daný produkt aktualizovať.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-aironet1

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 6.8**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Cisco IOS XE Software Ethernet Virtual Private Network Border Gateway Protocol Denial of Service Vulnerability

Popis

Zraniteľnosť v protokole Border Gateway Protocol (BGP) prostredníctvom Ethernet Virtual Private Network (EVPN) pre Cisco IOS XE Software by mohla umožniť neoverenému vzdialenému útočníkovi spôsobiť reštart zariadenia, čo by viedlo k neprístupnosti služby (DoS) alebo potenciálne poškodiť smerovaciu tabuľku BGP, čo by mohlo mať za následok nestabilitu siete.
Zraniteľnosť existuje v dôsledku zmien v implementácii BGP MPLS Based Ethernet VPN RFC (RFC 7432) medzi verziami softvéru IOS XE. Keď je prijatá aktualizácia paketu BGP Inclusive Multicast Ethernet Tag alebo BGP EVPN MAC / IP, je možné, že pole dĺžky IP adresy je nesprávne vypočítané. Útočník by túto chybu zabezpečenia mohol zneužiť odoslaním upraveného paketu BGP na postihnuté zariadenie po vytvorení relácie BGP.

Dátum prvého zverejnenia varovania

03. 11. 2017

CVE

CVE-2017-12319

Vendor ID (Cisco Bug ID)

CSCvg52875

Zasiahnuté systémy

Cisco IOS XE Software do 16.3, ktoré podporujú Border Gateway Protocol EVPN konfiguráciu

Následky

Neprístupnosť služby

Odporúčania

Spoločnosť Cisco vydala aktualizáciu na uvedený produkt, ktorá opravuje predmetnú zraniteľnosť. Odporúčame bezodkladne daný produkt aktualizovať.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171103-bgp

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 6.8**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Security updates for macOS High Sierra, Security Update 2017-001 Sierra, and Security Update 2017-004 El Capitan

Popis

Spoločnosť Apple vydala dôležitú aktualizáciu na produkty macOS High Sierra, Sierra a El Capitan, ktorá obsahuje niekoľko opráv dôležitých zraniteľností.
V novej verzii macOS High Sierra 10.13.1, v bezpečnostnej aktualizácii 2017-001 produktu Siera a v bezpečnostnej aktualizácii 2017-004 produktu El Capitan sa okrem iných rieši aj zraniteľnosť, označovaná ako KRACK, ktorá umožňovala rozšifrovať zašifrované WPA2 spojenie s prístupovým bodom.

Dátum prvého zverejnenia varovania

Prvé zverejnenie dňa 31. 10. 2017; aktualizácia dňa 03. 11. 2017

CVE

Kompletný zoznam CVE nájdete na: https://support.apple.com/en-us/HT208221

Zasiahnuté systémy

macOS High Sierra, Sierra a El Capitan

Následky

Neoprávnený prístup k informáciám

Odporúčania

Odporúčame bezodkladne aktualizovať macOS High Sierra, Sierra a El Capitan na najnovšie verzie a následne ich udržovať neustále aktualizované.

Zdroje

https://support.apple.com/en-us/HT208221

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 6.8**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Security updates for iOS

Popis

Spoločnosť Apple vydala dôležitú aktualizáciu na produkt iOS, ktorá obsahuje niekoľko opráv dôležitých zraniteľností.
V novej verzii 11.1 sa okrem iných rieši aj zraniteľnosť, označovaná ako KRACK, ktorá umožňovala rozšifrovať zašifrované WPA2 spojenie s prístupovým bodom.

Dátum prvého zverejnenia varovania

Prvé zverejnenie dňa 31. 10. 2017; aktualizácia dňa 03. 11. 2017

CVE

CVE-2017-13849, CVE-2017-13799, CVE-2017-13844, CVE-2017-13805, CVE-2017-13804, CVE-2017-7113, CVE-2017-13783, CVE-2017-13784, CVE-2017-13785, CVE-2017-13788, CVE-2017-13791, CVE-2017-13792, CVE-2017-13793, CVE-2017-13794, CVE-2017-13795, CVE-2017-13796, CVE-2017-13797, CVE-2017-13798, CVE-2017-13802, CVE-2017-13803, CVE-2017-13077, CVE-2017-13078, CVE-2017-13080

Zasiahnuté systémy

iOS vo verzii pred 11.1

Následky

Neoprávnený prístup k informáciám

Odporúčania

Odporúčame bezodkladne aktualizovať iOS na verziu 11.1 na vašich zariadeniach a následne ho udržovať neustále aktualizovaný.

Zdroje

https://support.apple.com/en-us/HT208222

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 6.3**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Security fixes in WordPress 4.8.3

Popis

Spoločnosť WordPress vydala aktualizáciu svojho redakčného systému na verziu 4.8.3, ktorá opravuje zraniteľnosť, umožňujúcu útok typu SQL Injection.
Predchádzajúce verzie Wordpress 4.8.2 a skoršie obsahujú problém, keď $wpdb->prepare() môže spôsobiť neočakávaný a nebezpečný dopyt vedúci k možnosti SQL injection. WordPress jadro nie je priamo ohrozené, ale v tejto aktualizácii sú obsiahnuté opravy, aby k tejto zraniteľnosti nedochádzalo zo strany pluginov a šablón.
Aktualizácia 4.8.3 takisto obsahuje zmeny v chovaní funkcie esc_sql().

Dátum prvého zverejnenia varovania

31. 10. 2017

CVE

CVE-2017-16510

Zasiahnuté systémy

WordPress vo verzii 4.8.2 a nižšie

Následky

Neoprávnené vykonanie škodlivého kódu, Neoprávnený prístup k informáciám

Odporúčania

Spoločnosť WordPress vydala aktualizáciu 4.8.3 na svoj redakčný systém, ktorý opravuje uvedenú zraniteľnosť, preto odporúčame aktualizovať tento produkt bezodkladne.

Zdroje

https://wordpress.org/news/2017/10/wordpress-4-8-3-security-release/
https://make.wordpress.org/core/2017/10/31/changed-behaviour-of-esc_sql-in-wordpress-4-8-3/
https://blog.ircmaxell.com/2017/10/disclosure-wordpress-wpdb-sql-injection-technical.html
https://blog.ircmaxell.com/2017/10/disclosure-wordpress-wpdb-sql-injection-background.html

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 4.8**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Falošná aplikácia WhatsApp na Google Play Store

Popis

Na oficiálnom obchode aplikácií pre operačný systém Android Google Play Store sa objavila falošná aplikácia komunikačnej platformy WhatsApp, ktorú si stiahlo viac ako milión používateľov.
Falošná aplikácia mala názov „Update WhatsApp Messenger“, pričom ako výrobca aplikácie bol uvedený oficiálny výrobca WhatsApp Inc.
Spoločnosť Google škodlivú aplikáciu ihneď odstránila z oficiálneho obchodu a taktiež zablokovalo aj účet falošného vývojára.

Dátum prvého zverejnenia varovania

01. 11. 2017

Vektor útoku

Útočníci využili na legitímne správanie aplikácie využili Unicode trik, keď za názov výrobcu aplikácie vložili medzeru vo forme špeciálneho znaku, pričom táto nie je v názve výrobcu aplikácie viditeľná. Aplikácia teda vyzerala, že je priamo od výrobcu WhatsApp.
Aplikácia vyžadovala len minimálne oprávnenia v zariadení, konkrétne vyžadovala iba pripojenie k internetu. Aplikácia sa v zariadeniach nezobrazovala, nakoľko nedisponovala ani názvom a ani ikonou, čo malo sťažiť jej odinštalovanie.
Po nainštalovaní aplikácie sa jej správanie prejavilo v zobrazovaní nežiaducej reklamy v zariadení, pričom neboli zaznamenané žiadne iné typy prípadných hrozieb zo strany tejto aplikácie.

Zasiahnuté systémy

Zariadenia s operačným systémom Android

Následky

Zobrazovanie nežiaduceho obsahu

Odporúčania

Odporúčame dodržiavať tieto opatrenia:

1. Ak využívate služby Google Play Store, pri sťahovaní aplikácii si riadne preverte výrobcu a účel aplikácie. Je to možné napríklad prostredníctvom oficiálnej stránky výrobcu aplikácie, kde sú zväčša uvedené všetky oficiálne aplikácie výrobcu.
2. Ak ste si nainštalovali vyššie uvedenú falošnú aplikáciu, odporúčame ihneď túto odinštalovať a to cez správu aplikácii v nastaveniach systému. Vyhľadajte aplikáciu, ktorá nemá logo ani názov a túto zmažte.
3. Takisto odporúčame pri využívaní služby Google Play Store využívať funkciu Google Play Protect, ktorá chráni používateľov pred sťahovaním škodlivých aplikácií.

Zdroje

https://thehackernews.com/2017/11/fake-whatsapp-android.html
https://motherboard.vice.com/en_us/article/evbakk/fake-whatsapp-android-app-1-million-downloads

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-022

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

Identifikátor

Security updates for iCloud for Windows 7.1

Popis

Spoločnosť Apple vydala dôležitú aktualizáciu na produkt iCloud pre Windows 7.1, ktorá obsahuje niekoľko opráv zraniteľností so strednou dôležitosťou.

Dátum prvého zverejnenia varovania

Prvé zverejnenie dňa 31. 10. 2017; aktualizácia dňa 02. 11. 2017

CVE

CVE-2017-13783, CVE-2017-13784, CVE-2017-13785, CVE-2017-13788, CVE-2017-13791, CVE-2017-13792, CVE-2017-13793, CVE-2017-13794, CVE-2017-13795, CVE-2017-13796, CVE-2017-13797, CVE-2017-13798, CVE-2017-13802, CVE-2017-13803

Zasiahnuté systémy

iCloud pre Windows 7.1

Následky

Neoprávnené vykonanie škodlivého kódu

Odporúčania

Odporúčame bezodkladne aktualizovať iCloud pre Windows 7.1 na vašich zariadeniach a následne ho udržovať neustále aktualizovaný.

Zdroje

https://support.apple.com/sk-sk/HT208225

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

Identifikátor

Security updates for Safari

Popis

Spoločnosť Apple vydala dôležitú aktualizáciu na produkt Safari, ktorá obsahuje niekoľko opráv zraniteľností so strednou dôležitosťou.

Dátum prvého zverejnenia varovania

Prvé zverejnenie dňa 31. 10. 2017; aktualizácia dňa 03. 11. 2017

CVE

CVE-2017-13790, CVE-2017-13789, CVE-2017-13783, CVE-2017-13784, CVE-2017-13785, CVE-2017-13788, CVE-2017-13791, CVE-2017-13792, CVE-2017-13793, CVE-2017-13794, CVE-2017-13795, CVE-2017-13796, CVE-2017-13797, CVE-2017-13798, CVE-2017-13802, CVE-2017-13803

Zasiahnuté systémy

Safari vo verzii pred 11.0.1

Následky

Neoprávnené vykonanie škodlivého kódu

Odporúčania

Odporúčame bezodkladne aktualizovať Safari na verziu 11.0.1 na vašich zariadeniach a následne ho udržovať neustále aktualizovaný.

Zdroje

https://support.apple.com/en-us/HT208223