BEZPEČNOSTNÝ BULLETIN

Týždeň 06. 02. 2019 - 12. 02. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava

Mail: sk-cert@nbu.gov.sk
Mobil: +421 903 993 706
Tel: +421 2 6869 2915

SK-CERT
Naša značka:
01380/2019/TS/OKB-039

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

Identifikátor

Zraniteľnosti Apple produktov

Popis

Spoločnosť Apple vydala bezpečnostné aktualizácie na svoje produkty macOS Mojave, iOS a Shortcuts ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

07.02.2019

CVE

CVE-2019-7289, CVE-2019-7290, CVE-2019-6223, CVE-2019-7286, CVE-2019-7287, CVE-2019-7288

Zasiahnuté systémy

macOS Mojave verzie staršie ako 10.14.3 Supplemental Update
iOS verzie staršie ako 12.1.4
Shortcuts verzie staršie ako 2.1.3 for iOS

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Eskalácia privilégií
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.apple.com/en-us/HT209522
https://support.apple.com/en-us/HT209521
https://support.apple.com/en-us/HT209520

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

Identifikátor

Simple DirectMedia Layer viacero zraniteľností

Popis

Vývojári knižnice Simple DirectMedia Layer informovali o viacerých bezpečnostných zraniteľnostiach vo svojom produkte.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

11.02.2019

CVE

CVE-2019-7636, CVE-2019-7635, CVE-2019-7573, CVE-2019-7572, CVE-2019-7577, CVE-2019-7638, CVE-2019-7637, CVE-2019-7574, CVE-2019-7576, CVE-2019-7575, CVE-2019-7578,

Zasiahnuté systémy

Simple DirectMedia Layer

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=59596
https://tools.cisco.com/security/center/viewAlert.x?alertId=59595
https://tools.cisco.com/security/center/viewAlert.x?alertId=59589
https://tools.cisco.com/security/center/viewAlert.x?alertId=59588
https://tools.cisco.com/security/center/viewAlert.x?alertId=59587
https://tools.cisco.com/security/center/viewAlert.x?alertId=59594
https://tools.cisco.com/security/center/viewAlert.x?alertId=59593
https://tools.cisco.com/security/center/viewAlert.x?alertId=59590
https://tools.cisco.com/security/center/viewAlert.x?alertId=59586
https://tools.cisco.com/security/center/viewAlert.x?alertId=59585
https://tools.cisco.com/security/center/viewAlert.x?alertId=59584

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

Identifikátor

Dell EMC VNX2 zraniteľnosť

Popis

Spoločnosť Dell vydala bezpečnostnú aktualizáciu na svoj produkt EMC VNX2, ktorá opravuje bezpečnostnú zraniteľnosť vo VNX Control Station.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciu bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá na napadnutom systéme.

Dátum prvého zverejnenia varovania

04.02.2019

CVE

CVE-2019-3704

Zasiahnuté systémy

Dell EMC VNX2verzie staršie ako 8.1.9.236

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://seclists.org/fulldisclosure/2019/Feb/8
https://exchange.xforce.ibmcloud.com/vulnerabilities/156601

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

Identifikátor

RunC zraniteľnosť

Popis

Vývojári nástroja pre správu kontajnerov RunC vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje lokálnemu útočníkovi vykonať škodlivý kód na hostiteľskom systéme s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

11.02.2019

CVE

CVE-2019-5736

Zasiahnuté systémy

Systémy pre správu kontajnerov založené na RunC

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.openwall.com/lists/oss-security/2019/02/11/2
https://access.redhat.com/security/cve/cve-2019-5736
https://www.redhat.com/en/blog/it-starts-linux-how-red-hat-helping-counter-linux-container-security-flaws
https://access.redhat.com/security/vulnerabilities/runcescape
https://aws.amazon.com/security/security-bulletins/AWS-2019-002/

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

Identifikátor

FreeRDP, rdesktop a Microsoft MSTSC viacero zraniteľností

Popis

Bezpečnostní výskumníci informovali o viacerých zraniteľnostiach v implementácii RDP protokolu v klientoch FreeRDP, rdesktop a Microsoft MSTSC.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočnou implementáciu bezpečnostných mechanizmov a umožňujú vzdialenému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

05.02.2019

CVE

CVE-2018-8791, CVE-2018-8792, CVE-2018-8793, CVE-2018-8794, CVE-2018-8795, CVE-2018-8796, CVE-2018-8797, CVE-2018-8798, CVE-2018-8799, CVE-2018-8800, CVE-2018-20174, CVE-2018-20175, CVE-2018-20176, CVE-2018-20177, CVE-2018-20178, CVE-2018-20179, CVE-2018-20180, CVE-2018-20181, CVE-2018-20182, CVE-2018-8784, CVE-2018-8785, CVE-2018-8786, CVE-2018-8787, CVE-2018-8788, CVE-2018-8789

Zasiahnuté systémy

Microsoft mstsc
FreeRDP verzie staršie ako 2.0.0-rc4
rdesktop verzie staršie ako v1.8.4

Následky

Vykonanie škodlivého kódu
Zneprístupnenie služby
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Používateľom Microsoft MSTSC odporúčame vypnúť funkciu obojstranného zdieľania obsahu schránky prostredníctvom RDP.

Zdroje

https://research.checkpoint.com/reverse-rdp-attack-code-execution-on-rdp-clients/
https://gbhackers.com/rdp-attack-critical-vulnerabilities/amp/

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

Identifikátor

Zraniteľnosti produktov Cisco

Popis

Viacero produktov od spoločnosti Cisco obsahuje bezpečnostné zraniteľnosti, ktoré sú spôsobené nesprávnym overovaním používateľských vstupov a nedostatočnou implementáciou bezpečnostných mechanizmov.
Najzávažnejšia bezpečnostná zraniteľnosť v produkte Cisco Aironet Active Sensor umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

06.02.2019

CVE

CVE-2019-1675, CVE-2019-1678, CVE-2019-1670, CVE-2019-1671, CVE-2019-1673, CVE-2019-1676, CVE-2019-1679, CVE-2019-1660, CVE-2019-1661, CVE-2019-1677, CVE-2019-1680, CVE-2019-1672

Zasiahnuté systémy

Cisco Aironet Active Sensor
Cisco Meeting Server
Cisco Unified Intelligence Center Software
Cisco Firepower Management Center
Cisco Identity Services Engine
Cisco Expressway Series Software
Cisco TelePresence Video Communication Server
Cisco TelePresence Conductor Software
Cisco TelePresence Management Suite
Cisco Webex Meetings for Android
Cisco Webex Business Suite
Cisco Web Security Appliance

Následky

Vykonanie škodlivého kódu
Zneprístupnenie služby
Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190206-wsa-bypass
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190206-webex-injection
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190206-webex-andro-xss
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190206-tms-xss
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190206-tms-soap
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190206-rest-api-ssrf
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190206-meeting-sipdos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190206-aas-creds
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190206-cms-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190206-cuic-xss
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190206-fmc-xss
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190206-ise-xss

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.3**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

cURL libcurl zraniteľnosti

Popis

Vývojári nástroja cURL (libcurl) vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť pretečenie zásobníka a vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

06.02.2019

CVE

CVE-2019-3822, CVE-2018-16890, CVE-2019-3823

Zasiahnuté systémy

libcurl verzie staršie ako 7.64.0

Následky

Vykonanie škodlivého kódu

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/156651
https://curl.haxx.se/docs/CVE-2019-3822.html
https://curl.haxx.se/docs/CVE-2019-3823.html
https://curl.haxx.se/docs/CVE-2018-16890.html

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 5.9
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Django framework zraniteľnosť

Popis

Vývojári webového frameworku Django vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú bezpečnostnú zraniteľnosť vo funkcii django.utils.numberformat.format() .
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

11.02.2019

CVE

CVE-2019-6975

Zasiahnuté systémy

Django 1.11.x verzie staršie ako 1.11.19, 2.0.x verzie staršie ako 2.0.11 a 2.1.x verzie staršie ako 2.1.6

Následky

Zneprístupnenie služby

Odporúčania

Odporúčame uistiť sa, či Vaše webové aplikácie nie sú založené na frameworku Django v zraniteľných verziách. V prípade, že áno, vykonajte aktualizáciu frameworku.

Zdroje

https://www.djangoproject.com/weblog/2019/feb/11/security-releases/
https://seclists.org/oss-sec/2019/q1/118
https://www.suse.com/security/cve/CVE-2019-6975/