BEZPEČNOSTNÝ BULLETIN

Týždeň 20. 03. 2019 - 26. 03. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	PuTTY viacero zraniteľností	Vysoká	**8.8**
02.	Mozilla Firefox viacero zraniteľností	Vysoká	**8.8**
03.	Mozilla Thunderbird zraniteľnosti	Vysoká	**8.8**
04.	Zraniteľnosti Apple produktov	Vysoká	**8.8**
05.	Kibana Elastic Stack zraniteľnosti	Vysoká	**8.8**
06.	SAP viacero zraniteľností	Vysoká	**8.7**
07.	Micro Focus ArcSight Logger zraniteľnosti	Vysoká	**8.4**
08.	IBM API Connect zraniteľnosť	Vysoká	**8.2**
09.	Cisco IP Phones viacero zraniteľností	Vysoká	**8.1**
10.	libssh2 viacero zraniteľností	Vysoká	**7.5**
11.	Zraniteľnosť bezdrôtovej myši Logitech M185	Vysoká	**7.5**
12.	Citrix Application Delivery Management zraniteľnosť	Vysoká	**7.5**
13.	F5 BIG-IP viacero zraniteľností	Vysoká	**7.5**
14.	XnView zraniteľnosti	Vysoká	**7.5**
15.	Ghostscript viacero zraniteľností	Vysoká	**7.3**
16.	SQLite viacero zraniteľností	Stredná	**6.5**
17.	Drupal zraniteľnosť	Stredná	**6.3**
18.	Moodle viacero zraniteľností	Stredná	**6.3**
19.	IBM Content Navigator zraniteľnosť	Stredná	**6.3**
20.	Zoho ManageEngine Netflow Analyzer Professional viacero zraniteľností	Stredná	**6.1**

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-091

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

Identifikátor

PuTTY viacero zraniteľností

Popis

Vývojári PuTTY vydali bezpečnostné aktualizácie na svoj produkt, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

16.03.2019

CVE

Zasiahnuté systémy

PuTTY verzie staršie ako 0.7.1

Následky

Neoprávnený prístup k citlivým údajom
Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://thehackernews.com/2019/03/putty-software-hacking.html
https://www.theregister.co.uk/2019/03/19/putty_patched_rsa_key_exchange_vuln/

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

Identifikátor

Mozilla Firefox viacero zraniteľností

Popis

Spoločnosť Mozilla vydala bezpečnostné aktualizácie, ktoré opravujú viacero zraniteľností v internetových prehliadačoch Firefox a Firefox ESR.
Najzávažnejšie bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

19.02.2019

CVE

CVE-2018-18506, CVE-2019-9788, CVE-2019-9789, CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9794, CVE-2019-9795, CVE-2019-9796, CVE-2019-9797, CVE-2019-9798, CVE-2019-9799, CVE-2019-9801, CVE-2019-9802, CVE-2019-9803, CVE-2019-9804, CVE-2019-9805, CVE-2019-9806, CVE-2019-9807, CVE-2019-9808, CVE-2019-9809, CVE-2019-9810, CVE-2019-9813

Zasiahnuté systémy

Mozilla Firefox staršie ako 66.0.1
Mozilla Firefox ESR staršie ako 60.6.1

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.mozilla.org/en-US/security/advisories/mfsa2019-10/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-09/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-08/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-07/

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

Identifikátor

Mozilla Thunderbird zraniteľnosti

Popis

Spoločnosť Mozilla vydala bezpečnostnú aktualizáciu na svoj produkt Thunderbird, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

25.03.2019

CVE

CVE-2019-9810, CVE-2019-9813

Zasiahnuté systémy

Mozilla Thunderbird verzie staršie ako 60.6.1

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.mozilla.org/en-US/security/advisories/mfsa2019-12/

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, Safari, iOS, tvOS, iCloud a iTunes, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi eskalovať svoje privilégiá na napadnutom systéme a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

25.03.2019

CVE

CVE-2018-12015, CVE-2018-18311, CVE-2018-18313, CVE-2018-4461, CVE-2019-6201, CVE-2019-6204, CVE-2019-6207, CVE-2019-6222, CVE-2019-6232, CVE-2019-6236, CVE-2019-6237, CVE-2019-6239, CVE-2019-7284, CVE-2019-7285, CVE-2019-7286, CVE-2019-7292, CVE-2019-7293, CVE-2019-8502, CVE-2019-8503, CVE-2019-8504, CVE-2019-8505, CVE-2019-8506, CVE-2019-8507, CVE-2019-8508, CVE-2019-8510, CVE-2019-8511, CVE-2019-8512, CVE-2019-8513, CVE-2019-8514, CVE-2019-8515, CVE-2019-8516, CVE-2019-8517, CVE-2019-8518, CVE-2019-8519, CVE-2019-8520, CVE-2019-8521, CVE-2019-8522, CVE-2019-8523, CVE-2019-8524, CVE-2019-8526, CVE-2019-8527, CVE-2019-8529, CVE-2019-8530, CVE-2019-8533, CVE-2019-8535, CVE-2019-8536, CVE-2019-8537, CVE-2019-8540, CVE-2019-8541, CVE-2019-8542, CVE-2019-8544, CVE-2019-8545, CVE-2019-8546, CVE-2019-8549, CVE-2019-8550, CVE-2019-8551, CVE-2019-8552, CVE-2019-8553, CVE-2019-8554, CVE-2019-8555, CVE-2019-8556, CVE-2019-8558, CVE-2019-8559, CVE-2019-8561, CVE-2019-8562, CVE-2019-8563, CVE-2019-8565, CVE-2019-8566, CVE-2019-8567

Zasiahnuté systémy

macOS Sierra 10.12.6, macOS High Sierra 10.13.6, macOS Mojave 10.14.3
Safari 12.1
iOS 12.2
tvOS 12.2
iCloud for Windows 7.11
iTunes 12.9.4 for Windows

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Zneprístupnenie služby
Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje
https://support.apple.com/en-us/HT209599
https://support.apple.com/en-us/HT209606
https://support.apple.com/en-us/HT209601
https://support.apple.com/en-us/HT209600
https://support.apple.com/en-us/HT209603
https://support.apple.com/en-us/HT209604
https://support.apple.com/en-us/HT209605

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

Identifikátor

Kibana Elastic Stack zraniteľnosti

Popis

Vývojári nástroja Kibana vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov a umožňujú vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

19.02.2019

CVE

CVE-2019-7608, CVE-2019-7609, CVE-2019-7610, CVE-2019-7611, CVE-2019-7612

Zasiahnuté systémy

Kibana verzie staršie ako 5.6.15 a 6.6.1

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://discuss.elastic.co/t/elastic-stack-6-6-1-and-5-6-15-security-update/169077
https://www.tenable.com/plugins/nessus/122589

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.7**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

SAP viacero zraniteľností

Popis

Spoločnosť SAP vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú viacero bezpečnostných zraniteľností. Najzávažnejšie z týchto zraniteľností umožňujú vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.03.2019

CVE

CVE-2018-2484, CVE-2018-7559, CVE-2019-0265, CVE-2019-0268, CVE-2019-0269, CVE-2019-0270, CVE-2019-0271, CVE-2019-0274, CVE-2019-0275, CVE-2019-0276, CVE-2019-0277

Zasiahnuté systémy

SAP Business Client verzia 6.5
SAP HANA Extended Application Services
SAP NetWeaver Java Application Server
ABAP Server
SAP Mobile Platform SDK
SAP BusinessObjects Business Intelligence Platform
SAP Plant Connectivity
SAP Enterprise Financial Services
Banking services from SAP, verzia 9.0

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=515408080

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.4
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Micro Focus ArcSight Logger zraniteľnosti

Popis

Spoločnosť Micro Focus vydala bezpečnostnú aktualizáciu na svoj produkt ArcSight Logger, ktorá opravuje 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

11.03.2019

CVE

CVE-2019-3479, CVE-2019-3480, CVE-2019-3481, CVE-2019-3482, CVE-2019-3483, CVE-2019-3484

Zasiahnuté systémy

Micro Focus ArcSight Logger verzie staršie ako 6.7

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://softwaresupport.softwaregrp.com/document/-/facetsearch/document/KM03355866

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.2**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

IBM API Connect zraniteľnosť

Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu na svoj produkt IBM API Connect, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k autentifikačným údajom.

Dátum prvého zverejnenia varovania

20.03.2019

CVE

CVE-2019-4052

Zasiahnuté systémy

IBM API Connect verzie staršie ako v2018.4.1.3

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www-01.ibm.com/support/docview.wss?uid=ibm10874248
https://nvd.nist.gov/vuln/detail/CVE-2019-4052

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

Identifikátor

Cisco IP Phones viacero zraniteľností

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na svoje IP telefóny, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia z týchto zraniteľností je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi nahrávať súbory na zariadenie.

Dátum prvého zverejnenia varovania

20.03.2019

CVE

CVE-2019-1716, CVE-2019-1763, CVE-2019-1764, CVE-2019-1765, CVE-2019-1766

Zasiahnuté systémy

Cisco Unified IP Conference Phone 8831 verzie staršie ako 10.3(1)SR5
Cisco Wireless IP Phone 8821 verzie staršie ako 8821-EX 11.0(4)SR3
Cisco IP Phone 7800 a 8800 verzie staršie ako 12.5(1)SR1

Následky

Neoprávnená zmena v systéme
Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190320-ipptv
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190320-ipfudos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190320-ipab
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190320-ip-phone-rce
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190320-ip-phone-csrf

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

Identifikátor

libssh2 viacero zraniteľností

Popis

Vývojári libssh2 vydali bezpečnostné aktualizácie na svoj produkt, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov a umožňujú vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

18.03.2019

CVE

CVE-2019-3855, CVE-2019-3856, CVE-2019-3857, CVE-2019-3858, CVE-2019-3859, CVE-2019-3860, CVE-2019-3861, CVE-2019-3862, CVE-2019-3863

Zasiahnuté systémy

libssh2 verzie staršie ako 1.8.1

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.libssh2.org/changes.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/158347
https://exchange.xforce.ibmcloud.com/vulnerabilities/158346
https://exchange.xforce.ibmcloud.com/vulnerabilities/158341
https://exchange.xforce.ibmcloud.com/vulnerabilities/158340
https://exchange.xforce.ibmcloud.com/vulnerabilities/158339
https://tools.cisco.com/security/center/viewAlert.x?alertId=59799
https://tools.cisco.com/security/center/viewAlert.x?alertId=59798
https://tools.cisco.com/security/center/viewAlert.x?alertId=59797

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-091

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

Identifikátor

Zraniteľnosť bezdrôtovej myši Logitech M185

Popis

Bezpečnostní výskumníci objavili zraniteľnosť v bezdrôtovej myši Logitech M185. Zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému útočníkovi v dosahu bezdrôtového prijímača pomocou špeciálne upravených paketov prevziať kontrolu nad myšou.

Dátum prvého zverejnenia varovania

18.03.2019

CVE

Zasiahnuté systémy

Bezdrôtová myš Logitech M185

Následky

Neoprávnený prístup do systému

Odporúčania

V súčasnej dobe na zraniteľnosť neexistuje bezpečnostná záplata.
Až do vydania aktualizácie odporúčame používať iný model myši.

Zdroje

https://www.davidsopas.com/popular-wireless-logitech-mouse-vulnerable-to-keystroke-injection/

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

Identifikátor

Citrix Application Delivery Management zraniteľnosť

Popis

Spoločnosť Citrix vydala bezpečnostnú aktualizáciu na svoj produkt Application Delivery Management, ktorá opravuje bezpečnostnú zraniteľnosť.
Bližšie nešpecifikovaná bezpečnostná zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

11.03.2019

CVE

CVE-2019-9548

Zasiahnuté systémy

Citrix Application Delivery Management verzie staršie ako 12.1 build 50.33
Citrix Application Delivery Management Agent Cloud verzie staršie ako 13.0 build 33

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://support.citrix.com/article/CTX247738

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-091

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

Identifikátor

F5 BIG-IP viacero zraniteľností

Popis

Spoločnosť F5 vydala bezpečnostnú aktualizáciu na svoj produkt BIG-IP, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

11.03.2019

CVE

CVE-2019-6596, CVE-2019-6601

Zasiahnuté systémy

BIG-IP verzie staršie ako 14.1.0, 14.0.0.3, 13.1.1.2, 12.1.4, 11.6.3.3, 11.5.9

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.f5.com/csp/article/K97241515
https://nvd.nist.gov/vuln/detail/CVE-2019-6596

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

Identifikátor

XnView zraniteľnosti

Popis

Bezpečnostní výskumníci informovali o viacerých bezpečnostných zraniteľnostiach v XnView Classic a XnView MP. Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov spôsobiť zneprístupnenie služieb

Dátum prvého zverejnenia varovania

21.03.2019

CVE

CVE-2019-9962, CVE-2019-9963, CVE-2019-9964, CVE-2019-9965, CVE-2019-9966, CVE-2019-9967, CVE-2019-9968, CVE-2019-9969

Zasiahnuté systémy

XnView Classic 2.48
XnView MP 0.93.1

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://code610.blogspot.com/2019/03/crashing-xnview-248.html

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

Identifikátor

Ghostscript viacero zraniteľností

Popis

Vývojári Artifex Software Ghostscript vydali bezpečnostnú aktualizáciu na ich produkt ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia z týchto zraniteľností je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

22.03.2019

CVE

CVE-2019-3835, CVE-2019-3838

Zasiahnuté systémy

v9.26 a staršie

Následky

Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.securityfocus.com/bid/107520/references
https://tools.cisco.com/security/center/viewAlert.x?alertId=59813
https://tools.cisco.com/security/center/viewAlert.x?alertId=59812

BEZPEČNOSTNÝ BULLETIN

Týždeň 20. 03. 2019 - 26. 03. 2019

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.5
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

SQLite viacero zraniteľností

Popis

Vývojári SQLite vydali bezpečnostnú aktualizáciu ktorá opravuje viacero bezpečnostných zraniteľností. Najzávažnejšia zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

22.03.2019

CVE

CVE-2019-9936, CVE-2019-9937

Zasiahnuté systémy

SQLite v3.27.2

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://nvd.nist.gov/vuln/detail/CVE-2019-9937
https://nvd.nist.gov/vuln/detail/CVE-2019-9936
https://tools.cisco.com/security/center/viewAlert.x?alertId=59815

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-091

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

Identifikátor

Drupal zraniteľnosť

Popis

Vývojári redakčného systému Drupal vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom cross-site scripting (XSS) útoku vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

20.03.2019

CVE

Zasiahnuté systémy

Drupal verzie staršie ako 8.6.13., 8.5.14. a 7.65

Následky

Vykonanie škodlivého kódu

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky nie sú založené na redakčnom systéme Drupal v zraniteľných verziách. V prípade že áno, zabezpečte aktualizáciu redakčného systému.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.drupal.org/sa-core-2019-004

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

Identifikátor

Moodle viacero zraniteľností

Popis

Vývojári Moodle vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi eskalovať svoje privilégiá.

Dátum prvého zverejnenia varovania

19.03.2019

CVE

CVE-2019-3847, CVE-2019-3848, CVE-2019-3849, CVE-2019-3850, CVE-2019-3851, CVE-2019-3852

Zasiahnuté systémy

Moodle verzie staršie ako 3.6.3, 3.5.5, 3.4.8 a 3.1.17

Následky

Eskalácia privilégií
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://moodle.org/mod/forum/discuss.php?d=384013
https://moodle.org/mod/forum/discuss.php?d=384010
https://moodle.org/mod/forum/discuss.php?d=384014
https://moodle.org/mod/forum/discuss.php?d=384012
https://www.cybersecurity-help.cz/vdb/SB2019031903

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

Identifikátor

IBM Content Navigator zraniteľnosť

Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu na svoj produkt Content Navigator, ktorá opravuje bezpečnostnú zraniteľnosť.
Bližšie nešpecifikovaná bezpečnostná zraniteľnosť umožňuje vzdialenému, autentifikovanému útočníkovi podvrhnúť škodlivý obsah.

Dátum prvého zverejnenia varovania

22.03.2019

CVE

CVE-2019-4035

Zasiahnuté systémy

IBM Content Navigator verzie staršie ako 3.0.4 iFix005 a 3.0.5 iFix001

Následky

Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www-01.ibm.com/support/docview.wss?uid=ibm10869060
https://nvd.nist.gov/vuln/detail/CVE-2019-4035
https://exchange.xforce.ibmcloud.com/vulnerabilities/156001

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.1
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Zoho ManageEngine Netflow Analyzer Professional viacero zraniteľností

Popis

Spoločnosť ManageEngine vydala bezpečnostnú aktualizáciu na svoj produkt Netflow Analyzer Professional, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňje vzdialenému, neautentifikovanému útočníkovi prostredníctvom Cross-Site Scripting (XSS) útoku získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

21.03.2019

CVE

CVE-2009-3903, CVE-2019-7422, CVE-2019-7423, CVE-2019-7424, CVE-2019-7425, CVE-2019-7426, CVE-2019-7427

Zasiahnuté systémy

v7.0.0.2

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://packetstormsecurity.com/files/151585/Zoho-ManageEngine-Netflow-Analyzer-Professional-7.0.0.2-XSS.html
https://nvd.nist.gov/vuln/detail/CVE-2019-7422
https://nvd.nist.gov/vuln/detail/CVE-2019-7424

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-091