BEZPEČNOSTNÝ BULLETIN

Týždeň 17. 07. 2019 - 23. 07. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Zraniteľnosť Drupal CMS	Vysoká	**8.8**
02.	Zraniteľnosti Apple produktov	Vysoká	**8.8**
03.	GNOME Evince zraniteľnosť	Vysoká	**8.8**
04.	PaloAlto zraniteľnosť	Vysoká	**8.1**
05.	Comodo Antivirus viacero zraniteľností	Vysoká	**7.8**
06.	libssh2 zraniteľnosť	Vysoká	**7.5**
07.	Foxit Software Foxit PhantomPDF zraniteľnosti	Vysoká	**7.5**
08.	Johnson Controls exacqVision Server zraniteľnosť	Stredná	**6.7**
09.	Jenkins viacero zraniteľností	Stredná	**6.0**

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-189

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

Identifikátor

Zraniteľnosť Drupal CMS

Popis

Vývojári redakčného systému Drupal vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť v komponente Workspaces umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

17.07.2019

CVE

CVE-2019-6342

Zasiahnuté systémy

Drupal 8.7.4.

Následky

Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.drupal.org/sa-core-2019-008
https://www.bleepingcomputer.com/news/security/drupal-patches-critical-bug-that-lets-hackers-take-over-sites/

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 a watchOS, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti 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

22.07.2019

CVE

CVE-2018-16860, CVE-2019-13118, CVE-2019-8641, CVE-2019-8644, CVE-2019-8646, CVE-2019-8647, CVE-2019-8649, CVE-2019-8657, CVE-2019-8658, CVE-2019-8660, CVE-2019-8662, CVE-2019-8666, CVE-2019-8669, CVE-2019-8671, CVE-2019-8672, CVE-2019-8673, CVE-2019-8676, CVE-2019-8677, CVE-2019-8678, CVE-2019-8679, CVE-2019-8680, CVE-2019-8681, CVE-2019-8683, CVE-2019-8684, CVE-2019-8685, CVE-2019-8686, CVE-2019-8687, CVE-2019-8688, CVE-2019-8689, CVE-2019-8690, CVE-2019-8698

Zasiahnuté systémy

macOS Mojave 10.14.6, Security Update 2019-004 High Sierra, Security Update 2019-004 Sierra
Safari verzie staršie ako 12.1.2
iOS verzie staršie ako 12.4
tvOS verzie staršie ako 12.4
watchOS verzie staršie ako 5.3

Následky

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

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.cisecurity.org/advisory/multiple-vulnerabilities-in-apple-products-could-allow-for-arbitrary-code-execution_2019-074/ https://support.apple.com/en-us/HT210346 https://support.apple.com/en-us/HT210348 https://support.apple.com/en-us/HT210351 https://support.apple.com/en-us/HT210353 https://support.apple.com/en-us/HT210355

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

Identifikátor

GNOME Evince zraniteľnosť

Popis

Vývojári Linux prostredia GNOME vydali bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť v prehliadači PDF dokumentov Evince.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného PDF súboru vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému alebo spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

18.07.2019

CVE

CVE-2019-1010006

Zasiahnuté systémy

The GNOME Project verzia 3.26

Následky

Zneprístupnenie služby

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.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=60475
https://bug788980.bugzilla-attachments.gnome.org/attachment.cgi?id=365866

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

Identifikátor

PaloAlto zraniteľnosť

Popis

Spoločnosť PaloAlto Networks vydala bezpečnostnú aktualizáciu na svoj produkt PAN-OS, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

19.07.2019

CVE

CVE-2019-1579

Zasiahnuté systémy

PAN-OS verzie staršie ako 7.1.19
PAN-OS verzie staršie ako 8.0.12
PAN-OS verzie staršie ako 8.1.3

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne 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://nvd.nist.gov/vuln/detail/CVE-2019-1579
http://blog.orange.tw/2019/07/attacking-ssl-vpn-part-1-preauth-rce-on-palo-alto.html
https://securityadvisories.paloaltonetworks.com/(X(1)S(cai35yxwa4kjktang3j4eu1e))/Home/Detail/158

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

Identifikátor

Comodo Antivirus viacero zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o bezpečnostnej zraniteľnosti v produkte Comodo Antivirus.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi eskalovať svoje privilégiá. Proof-of-concept (PoC) kód je verejne dostupný.

Dátum prvého zverejnenia varovania

16.07.2019

CVE

CVE-2019-3969, CVE-2019-3970, CVE-2019-3971, CVE-2019-3972, CVE-2019-3973

Zasiahnuté systémy

Comodo Antivirus verzie staršie ako 12.0.0.6810

Následky

Neoprávnená zmena v systéme
Zneprístupnenie služby
Eskalácia privilégií

Odporúčania

Na uvedené zraniteľnosti v súčasnosti nie sú dostupné aktualizácie. Administrátorom odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.

Zdroje

https://www.tenable.com/security/research/tra-2019-34

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

Identifikátor

libssh2 zraniteľnosť

Popis

Vývojári knižnice libssh2 vydali bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť vo funkcii kex_method_diffie_hellman_group_exchange_sha256_key_exchange.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi, vydávajúcemu sa za SSH server, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému alebo spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

18.07.2019

CVE

CVE-2019-13115

Zasiahnuté systémy

libssh2 verzie staršie ako 1.9.0

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=60480
https://libssh2.org/changes.html

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

Identifikátor

Foxit Software Foxit PhantomPDF zraniteľnosti

Popis

Spoločnosť Foxit Software vydala bezpečnostné aktualizácie na svoj produkt Foxit PhantomPDF, ktorá opravuje viacero bezpečnostných zraniteľností.
Uvedené zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného PDF súboru vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

19.07.2019

CVE

CVE-2019-14207, CVE-2019-14208, CVE-2019-14209, CVE-2019-14210, CVE-2019-14211, CVE-2019-14212, CVE-2019-14213, CVE-2019-14214, CVE-2019-14215

Zasiahnuté systémy

Foxit PhantomPDF verzie staršie ako 8.3.11

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.

Zdroje

https://www.foxitsoftware.com/support/security-bulletins.php
https://nvd.nist.gov/vuln/detail/CVE-2019-14215
https://nvd.nist.gov/vuln/detail/CVE-2019-14214
https://nvd.nist.gov/vuln/detail/CVE-2019-14213
https://nvd.nist.gov/vuln/detail/CVE-2019-14212
https://nvd.nist.gov/vuln/detail/CVE-2019-14211
https://nvd.nist.gov/vuln/detail/CVE-2019-14210
https://nvd.nist.gov/vuln/detail/CVE-2019-14209
https://nvd.nist.gov/vuln/detail/CVE-2019-14208
https://nvd.nist.gov/vuln/detail/CVE-2019-14207

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.7
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Johnson Controls exacqVision Server zraniteľnosť

Popis

Spoločnosť Johnson Controls vydala bezpečnostnú aktualizáciu na svoj produkt exacqVision Server, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

18.07.2019

CVE

CVE-2019-7590

Zasiahnuté systémy

Johnson Controls exacqVision Server verzie staršie ako 19.03

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://www.us-cert.gov/ics/advisories/icsa-19-199-01

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.0
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Jenkins viacero zraniteľností

Popis

Vývojári software Jenkins vydali bezpečnostné aktualizácie, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

17.07.2019

CVE

CVE-2019-10352, CVE-2019-10353, CVE-2019-10354

Zasiahnuté systémy

Jenkins weekly verzie staršie ako 2.146
Jenkins LTS verzie staršie ako 2.138.2

Následky

Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov a limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje

https://www.tenable.com/security/research/tra-2019-35
https://jenkins.io/security/advisory/2019-07-17/#SECURITY-1424