BEZPEČNOSTNÝ BULLETIN

Týždeň 14. 08. 2019 - 20. 08. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Cisco Nexus 9000 zraniteľnosť	Vysoká	**8.8**
02.	OpenCV zraniteľnosti	Vysoká	**8.2**
03.	Linux Kernel zraniteľnosti	Vysoká	**8.0**
04.	PostgreSQL zraniteľnosti	Vysoká	**7.8**
05.	LibreOffice zraniteľnosti	Vysoká	**7.8**
06.	Fuji Electric Alpha5 Smart Loader zraniteľnosť	Vysoká	**7.8**
07.	Cisco Jabber zraniteľnosť	Vysoká	**7.3**
08.	McAfee Web Gateway zraniteľnosti	Vysoká	**7.1**
09.	Johnson Controls Metasys zraniteľnosť	Stredná	**6.8**
10.	Cisco Firepower Threat Defence zraniteľnosti	Stredná	**5.8**

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-206

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

Identifikátor

Cisco Nexus 9000 zraniteľnosť

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie, ktoré opravujú bezpečnostnú zraniteľnosť v produkte Cisco Nexus 9000.
Zraniteľnosť spočíva v nedostatočnom overovaní vybraných polí hlavičky LLDP rámca v LLDP (Link Layer Discovery Protocol) podsystéme a neautentifikovaný útočník v rovnakom sieťovom segmente by ju prostredníctvom podvrhnutia špeciálne vytvorených LLDP paketov mohol zneužiť na vykonanie škodlivého kódu alebo zneprístupnenie služby.

Dátum prvého zverejnenia varovania

16.08.2019

CVE

CVE-2019-1901

Zasiahnuté systémy

Cisco Nexus 9000 Series ACI Mode Switch Software verzie staršie ako 13.2(7f) a 14.1(2m)

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190731-nxos-bo

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

Identifikátor

OpenCV zraniteľnosti

Popis

Vývojári knižnice OpenCV vydali aktualizáciu, ktorá opravuje viacero bezpečnostných zraniteľností. Bezpečnostné zraniteľnosti spočívajú v implementačných chybách vo funkciách cv::predictOrdered, HaarEvaluator::OptFeature::calc, cv::XMLParser::parse a vzdialený neautentifikovaný útočník by ich prostredníctvom špeciálne vytvorených požiadaviek mohol zneužiť na zneprístupnenie služby.

Dátum prvého zverejnenia varovania

14.08.2019

CVE

CVE-2019-14491, CVE-2019-14492, CVE-2019-14493

Zasiahnuté systémy

OpenCV verzie staršie ako 3.4.7
OpenCV verzie staršie ako 4.1.1

Následky

Zneprístupnenie služby

Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie a produkty nevyužívajú knižnicu OpenCV. V prípade, že áno, administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=60574
https://tools.cisco.com/security/center/viewAlert.x?alertId=60573
https://tools.cisco.com/security/center/viewAlert.x?alertId=60576

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.0**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Linux Kernel zraniteľnosti

Popis

Vývojári Linux Kernel vydali bezpečnostné aktualizácie, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia zraniteľnosť sa nachádza vo funkcii bc_svc_process() v NFS41+ subsystéme a autentifikovaný útočník v rovnakom sieťovom segmente by ju mohol zneužiť na vykonanie škodlivého kódu alebo znneprístupnenie služby.
Ostatné zraniteľnosti v drivers/usb/dwc3/gadget.c, drivers/usb/gadget/function/f_midi.cby a mixer.c by lokálny autentifikovaný útočník mohol zneužiť na znneprístupnenie služby.

Dátum prvého zverejnenia varovania

16.08.2019

CVE

CVE-2018-16884, CVE-2018-20961, CVE-2019-14763, CVE-2019-15117

Zasiahnuté systémy

Linux Kernel verzie 4.16.3 a staršie

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Znneprístupnenie 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://tools.cisco.com/security/center/viewAlert.x?alertId=60584
https://tools.cisco.com/security/center/viewAlert.x?alertId=60581
https://tools.cisco.com/security/center/viewAlert.x?alertId=60596
https://exchange.xforce.ibmcloud.com/vulnerabilities/165425
https://cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.16.4
https://patchwork.kernel.org/cover/10733767/

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

Identifikátor

PostgreSQL zraniteľnosti

Popis

Vývojári databázového systému PostgreSQL vydali aktualizácie na svoj produkt, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšiu zraniteľnosť by lokálny autentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvoreného OpenSSL konfiguračného súbora pre EnterpriseDB Windows inštalátor mohol zneužiť na vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.
Ostatné zraniteľnosti by vzdialený autentifikovaný útočník mohol zneužiť na vykonanie SQL príkazov a následne zobraziť, pridať, upraviť alebo odstrániť údaje uložené v databáze.

Dátum prvého zverejnenia varovania

15.08.2019

CVE

CVE-2019-10208, CVE-2019-10209, CVE-2019-10211

Zasiahnuté systémy

PostgreSQL verzie 11.4 a staršie

Následky

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

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://tools.cisco.com/security/center/viewAlert.x?alertId=60586
https://tools.cisco.com/security/center/viewAlert.x?alertId=60585
https://tools.cisco.com/security/center/viewAlert.x?alertId=60588

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

Identifikátor

LibreOffice zraniteľnosti

Popis

Vývojári kancelárskeho balíka LibreOffice vydali aktualizáciu svojho produktu, ktorá opravuje viaceré bezpečnostné zraniteľnosti.
Zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a vzdialený neautentifikovaný útočník by ich prostredníctvom podvrhnutia špeciálne vytvorených súborov mohol zneužiť na vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.08.2019

CVE

CVE-2019-9850, CVE-2019-9851, CVE-2019-9852

Zasiahnuté systémy

LibreOffice verzie staršie ako 6.2.6
LibreOffice verzie staršie ako 6.3.0

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.libreoffice.org/about-us/security/advisories/cve-2019-9850/
https://www.libreoffice.org/about-us/security/advisories/cve-2019-9851/
https://www.libreoffice.org/about-us/security/advisories/cve-2019-9852/
https://exchange.xforce.ibmcloud.com/vulnerabilities/165422
https://exchange.xforce.ibmcloud.com/vulnerabilities/165423
https://exchange.xforce.ibmcloud.com/vulnerabilities/165424

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

Identifikátor

Fuji Electric Alpha5 Smart Loader zraniteľnosť

Popis

Spoločnosť Fuji Electric vydala bezpečnostné aktualizácie, ktoré opravujú bezpečnostnú zraniteľnosť v produkte Alpha5 Smart Loader.
Bližšie nešpecifikovanú zraniteľnosť by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvorených Project súborov mohol zneužiť na vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.08.2019

CVE

CVE-2019-13520

Zasiahnuté systémy

Alpha5 Smart Loader verzie staršie ako 4.2

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.us-cert.gov/ics/advisories/icsa-19-227-02

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

Identifikátor

Cisco Jabber zraniteľnosť

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie, ktoré opravujú bezpečnostnú zraniteľnosť v produkte Cisco Jabber.
Zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a lokálny autentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvoreného DLL súboru mohol zneužiť na vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

19.08.2019

CVE

CVE-2019-1855

Zasiahnuté systémy

Cisco Jabber pre Windows verzie staršie ako 12.6.2

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-jabber-dll

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.1
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

McAfee Web Gateway zraniteľnosti

Popis

Spoločnosť McAfee vydala bezpečnostné aktualizácie, ktoré opravujú dve bezpečnostné zraniteľnosti v produkte Web Gateway.
Bezpečnostné zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a vzdialený útočník by ju mohol zneužiť na získanie neoprávneného prístupu k citlivým údajom.

Dátum prvého zverejnenia varovania

13.08.2019

CVE

CVE-2019-3635, CVE-2019-3639

Zasiahnuté systémy

MWG 7.7.2 staršie ako MWG 7.7.2.23; MWG 7.8.2 staršie ako MWG 7.8.2.12; MGW 8.x staršie ako 8.1.5 (CVE-2019-3635)
MWG 7.8.2 staršie ako MWG 7.8.2.12; MWG 8.x staršie ako 8.1.5 (CVE-2019-3639)

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Taktiež odporúčame poučiť používateľov, aby neotvárali linky z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://kc.mcafee.com/corporate/index?page=content&id=SB10293
https://exchange.xforce.ibmcloud.com/vulnerabilities/165313
https://exchange.xforce.ibmcloud.com/vulnerabilities/165315

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

Identifikátor

Johnson Controls Metasys zraniteľnosť

Popis

Spoločnosť Johnson Controls vydala bezpečnostné aktualizácie, ktoré opravujú bezpečnostné zraniteľnosti v produkte Metasys.
Bezpečnostné zraniteľnosti spočívajú v existencii zabudovaných RSA a RC2 kľúčových párov pre šifrovacie operácie vykonávané prostredníctvom SMP (Site Management Portal). Zraniteľnosti by vzdialený neautentifikovaný útočník s prístupom k daným kľúčom mohol zneužiť na dešifrovanie komunikácie medzi Metasys ADS/ADX servermi a SMP klientom pripájajúcich sa používateľov a získať tak neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

15.08.2019

CVE

CVE-2019-7593, CVE-2019-7594

Zasiahnuté systémy

Metasys system verzie staršie ako 9.0

Následky

Neoprávnený prístup k citlivým údajom

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-19-227-01

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 5.8
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Cisco Firepower Threat Defence zraniteľnosti

Popis

Spoločnosť Cisco zverejnila informácie o bezpečnostných zraniteľnostiach v produkte Cisco Firepower Threat Defence.
Zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a vzdialený neautentifikovaný útočník by ich prostredníctvom podvrhnutia špeciálne vytvorených požiadaviek a sieťovej prevádzky mohol zneužiť na obídenie filtračných pravidiel zariadenia, podvrhnutie škodlivého obsahu a následné získanie neoprávneného prístupu do systému.

Dátum prvého zverejnenia varovania

16.08.2019

CVE

CVE-2019-1978, CVE-2019-1980, CVE-2019-1981, CVE-2019-1982

Zasiahnuté systémy

Cisco Firepower Threat Defense Software
Cisco Firepower Services Software for ASA
Cisco Firepower Management Center Software

Následky

Neoprávnený prístup do systému

Odporúčania

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

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190816-ftd-http
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190816-ftd-nspd
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190816-ftd-null
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190816-ftd-srb

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-206