BEZPEČNOSTNÝ BULLETIN

Týždeň 21. 08. 2019 – 27. 08. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Google Chrome viacero zraniteľností	Vysoká	**8.8**
02.	Zraniteľnosti tlačiarní Ricoh	Vysoká	**8.8**
03.	Apple iOS, tvOS, macOS zraniteľnosť	Vysoká	**8.8**
04.	Schneider Electric spaceLYnk & homeLYnk zraniteľnosť	Vysoká	**8.3**
05.	IBM Security Access Manager zraniteľnosť	Vysoká	**8.2**
06.	Apache HTTP Server zraniteľnosti	Vysoká	**8.1**
07.	IBM Security Guardium zraniteľnosť	Vysoká	**7.1**
08.	IBM Business Automation Workflow a BPM zraniteľnosť	Vysoká	**7.1**
09.	OpenEMR zraniteľnosti	Stredná	**6.5**

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-209

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

Identifikátor

Google Chrome viacero zraniteľností

Popis

Spoločnosť Google vydala aktualizáciu na svoj internetový prehliadač Google Chrome, ktorá opravuje trojicu bezpečnostných zraniteľností.
Najzávažnejšia z týchto zraniteľností v komponente Blink umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

26.08.2019

CVE

CVE-2019-5869

Zasiahnuté systémy

Google Chrome verzie staršie ako 76.0.3809.132

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://chromereleases.googleblog.com/2019/08/stable-channel-update-for-desktop_26.html

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

Identifikátor

Zraniteľnosti tlačiarní Ricoh

Popis

Spoločnosť Ricoh vydala bezpečnostnú aktualizáciu na svoje tlačiarne SP C250SF, SP C252SF, SP C250DN a SP C252DN, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

23.08.2019

CVE

CVE-2019-14300, CVE-2019-14305, CVE-2019-14307, CVE-2019-14308

Zasiahnuté systémy

Ricoh SP C250SF a SP C252SF firmware verzie staršie ako 1.07
Ricoh SP C250DN a SP C252DN firmware verzie staršie ako 1.13

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://www.ricoh.com/info/2019/0823_1/

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

Identifikátor

Apple iOS, tvOS, macOS zraniteľnosť

Popis

Spoločnosť Apple vydala bezpečnostnú aktualizáciu na svoje produkty iOS, tvOS a macOS Mojave ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov eskalovať svoje privilégiá na zasiahnutom systéme.

Dátum prvého zverejnenia varovania

26.08.2019

CVE

CVE-2019-8605

Zasiahnuté systémy

Apple iOS verzie staršie ako 12.4.1
Apple tvOS verzie staršie ako 12.4.1
Apple macOS Mojave verzie staršie ako 10.14.6

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a neinštalovali nedôveryhodné aplikácie.

Zdroje

https://support.apple.com/en-us/HT210549
https://support.apple.com/en-us/HT210548
https://support.apple.com/en-us/HT210550
https://www.theregister.co.uk/2019/08/26/apple_fixes_ios124_jailbreak/
https://www.bleepingcomputer.com/news/security/apple-releases-ios-1241-to-patch-security-flaw-behind-jailbreak/
https://www.tenable.com/plugins/nessus/128150

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.3**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Schneider Electric spaceLYnk & homeLYnk zraniteľnosť

Popis

Spoločnosť Schneider Electric vydala bezpečnostnú aktualizáciu na svoje produkty spaceLYnk & homeLYnk ktorá opravuje bezpečnostnú zraniteľnosť.
Bližšie nešpecifikovaná bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

13.08.2019

CVE

CVE-2019-6832

Zasiahnuté systémy

spaceLYnk verzie staršie ako 2.4.0
Wiser for KNX (homeLYnk) verzie staršie ako 2.4.0

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do systému
Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.
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://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SEVD-2019-225-07-spaceLYnk-homeLYnk.pdf&p_Doc_Ref=SEVD-2019-225-07

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

Identifikátor

IBM Security Access Manager zraniteľnosť

Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu na svoj produkt Security Access Manager, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených XML súborov získať prístup k citlivým údajom a spôsobiť odopretie služieb.

Dátum prvého zverejnenia varovania

21.08.2019

CVE

CVE-2019-4513

Zasiahnuté systémy

IBM Security Access Manager for Enterprise Single Sign-On 8.2.2

Následky

Neoprávnený prístup k citlivým údajom
Zneprístupnenie služby

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=ibm10996716
https://exchange.xforce.ibmcloud.com/vulnerabilities/164555
https://nvd.nist.gov/vuln/detail/CVE-2019-4513

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

Identifikátor

Apache HTTP Server zraniteľnosti

Popis

Vývojári systému Apache HTTP Server vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť pretečenie zásobníka a následne vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

14.08.2019

CVE

CVE-2019-10081, CVE-2019-10097, CVE-2019-10082, CVE-2019-10092, CVE-2019-9517, CVE-2019-10098

Zasiahnuté systémy

Apache HTTP Server verzie staršie ako 2.4.41

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Zneprístupnenie služby
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://httpd.apache.org/security/vulnerabilities_24.html
https://tools.cisco.com/security/center/viewAlert.x?alertId=60638
https://tools.cisco.com/security/center/viewAlert.x?alertId=60637
https://tools.cisco.com/security/center/viewAlert.x?alertId=60640
https://tools.cisco.com/security/center/viewAlert.x?alertId=60641
https://tools.cisco.com/security/center/viewAlert.x?alertId=60639
https://tools.cisco.com/security/center/viewAlert.x?alertId=60642

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

Identifikátor

IBM Security Guardium zraniteľnosť

Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu na svoj produkt Security Guardium, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených XML súborov získať prístup k citlivým údajom a spôsobiť odopretie služieb.

Dátum prvého zverejnenia varovania

16.08.2019

CVE

CVE-2019-4340

Zasiahnuté systémy

IBM Security Guardium Big Data Intelligence 4.0

Následky

Neoprávnený prístup k citlivým údajom
Zneprístupnenie služby

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=ibm10960856
https://exchange.xforce.ibmcloud.com/vulnerabilities/161419

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

Identifikátor

IBM Business Automation Workflow a BPM zraniteľnosť

Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu na svoje produkty Business Automation Workflow a BPM, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených XML súborov získať prístup k citlivým údajom a spôsobiť odopretie služieb.

Dátum prvého zverejnenia varovania

06.08.2019

CVE

CVE-2019-4424

Zasiahnuté systémy

IBM Business Automation Workflow verzie staršie ako V19.0.0.3
IBM Business Process Manager

Následky

Neoprávnený prístup k citlivým údajom
Zneprístupnenie služby

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=ibm10959537
https://exchange.xforce.ibmcloud.com/vulnerabilities/162770

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

Identifikátor

OpenEMR zraniteľnosti

Popis

Vývojári systému pre správu zdravotníckych informácií OpenEMR vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti spočívajú v nedostatočnom overovaní používateľských vstupov zasiahnutým systémom a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom cross-site scripting útoku vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

19.08.2019

CVE

CVE-2019-3963, CVE-2019-3964, CVE-2019-3965, CVE-2019-3966, CVE-2019-3967, CVE-2019-3968, CVE-2019-14530

Zasiahnuté systémy

OpenEMR verzie staršie ako 5.0.2.

Následky

Vykonanie škodlivého kódu
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://www.tenable.com/security/research/tra-2019-40
https://tools.cisco.com/security/center/viewAlert.x?alertId=60626