BEZPEČNOSTNÝ BULLETIN

Týždeň 19. 08. 2020 - 25. 08. 2020

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Google Chrome - zraniteľnosť	Vysoká	**8.8**
02.	Moxa NPort IAW5000A-I/O Series Serial Device Servers - zraniteľnosti	Vysoká	**8.8**
03.	Foxit Studio Photo - viacero zraniteľností	Vysoká	**8.8**
04.	NCR SelfServ bankomaty - viacero zraniteľností	Vysoká	**7.6**
05.	BIND - viacero zraniteľností	Stredná	**6.7**
06.	IBM Security Guardium Insights - viacero zraniteľností	Stredná	**6.5**
07.	Diebold Nixdorf 2100xe USB bankomaty - zraniteľnosť	Stredná	**5.4**

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:
01439/2020/SK-CERT-211

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

Identifikátor

Google Chrome - zraniteľnosť

Popis

Spoločnosť Google vydala aktualizáciu na svoj internetový prehliadač Google Chrome, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť v komponente SwiftShader umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upraveného webového obsahu spôsobiť pretečenie zásobníka a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

18.08.2020

CVE

CVE-2020-6556

Zasiahnuté systémy

Google Chrome verzie staršie ako 84.0.4147.135

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/2020/08/stable-channel-update-for-desktop_18.html
https://www.cisecurity.org/advisory/a-vulnerability-in-google-chrome-could-allow-for-arbitrary-code-execution_2020-118/

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

Identifikátor

Moxa NPort IAW5000A-I/O Series Serial Device Servers - zraniteľnosti

Popis

Spoločnosť Moxa vydala aktualizáciu na svoj produkt NPort IAW5000A-I/O Series Serial Device Servers, ktorá opravuje viacero bezpečnostných zraniteľností.
Bližšie nešpecifikované bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi eskalovať svoje privilégiá a získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

20.08.2020

CVE

-

Zasiahnuté systémy

Moxa NPort IAW5000A-I/O Series Serial Device Servers firmvér verzie staršie ako 2.2

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://www.moxa.com/en/support/support/security-advisory/nport-iaw5000a-io-serial-device-servers-vulnerabilities

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

Identifikátor

Foxit Studio Photo - viacero zraniteľností

Popis

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

Dátum prvého zverejnenia varovania

21.08.2020

CVE

CVE-2020-17403, CVE-2020-17404

Zasiahnuté systémy

Foxit Studio Photo verzie staršie ako 3.6.6.928

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.foxitsoftware.com/support/security-bulletins.html
https://www.zerodayinitiative.com/advisories/ZDI-20-1079/
https://www.zerodayinitiative.com/advisories/ZDI-20-1078/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.6
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

NCR SelfServ bankomaty - viacero zraniteľností

Popis

Spoločnosť NCR vydala aktualizáciu na svoje SelfServ bankomaty, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú neautentifikovanému útočníkovi s fyzickým prístupom k zariadeniu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

20.08.2020

CVE

CVE-2020-10123, CVE-2020-10124, CVE-2020-10125, CVE-2020-10126, CVE-2020-9063

Zasiahnuté systémy

NCR SelfServ ATMs APTRA XFS verzie staršie ako 06.08

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Taktiež odporúčame zabezpečiť systém podľa odporúčaní výrobcu.

Zdroje

https://www.kb.cert.org/vuls/id/116713
https://www.ncr.com/content/dam/web/documents/banking-endpoint-security/NCR%20Security%20Alert%20-%202020-05%20Black%20Box%20Attachs%20in%20Europe.pdf
https://www.ncr.com/content/dam/ncrcom/content-type/documents/NCR_Secure_white_paper-Dispenser_Security_Solution_September_2018.pdf
https://exchange.xforce.ibmcloud.com/vulnerabilities/187013
https://exchange.xforce.ibmcloud.com/vulnerabilities/187012
https://exchange.xforce.ibmcloud.com/vulnerabilities/187014
https://exchange.xforce.ibmcloud.com/vulnerabilities/187016
https://exchange.xforce.ibmcloud.com/vulnerabilities/187017

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

Identifikátor

BIND - viacero zraniteľností

Popis

Vývojári DNS servera BIND vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti spočívajú v nedostatočnom overovaní používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených požiadaviek spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

20.08.2020

CVE

CVE-2020-8620, CVE-2020-8621, CVE-2020-8622, CVE-2020-8623, CVE-2020-8624

Zasiahnuté systémy

BIND verzie staršie ako 9.16.6 a 9.17.4

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://us-cert.cisa.gov/ncas/current-activity/2020/08/21/isc-releases-security-advisories-bind
https://talosintelligence.com/vulnerability_reports/TALOS-2020-1100
https://kb.isc.org/docs/cve-2020-8620
https://kb.isc.org/docs/cve-2020-8621
https://kb.isc.org/docs/cve-2020-8622
https://kb.isc.org/docs/cve-2020-8623
https://kb.isc.org/docs/cve-2020-8624

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

Identifikátor

IBM Security Guardium Insights - viacero zraniteľností

Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu na svoj produkt Security Guardium Insights, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

20.08.2020

CVE

CVE-2020-4165, CVE-2020-4598

Zasiahnuté systémy

IBM Security Guardium Insights verzia 2.0.1

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.ibm.com/support/pages/node/6320061
https://www.ibm.com/support/pages/node/6320069
https://exchange.xforce.ibmcloud.com/vulnerabilities/184823

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 5.4
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Diebold Nixdorf 2100xe USB bankomaty - zraniteľnosť

Popis

Spoločnosť Diebold Nixdorf vydala aktualizáciu na svoje bankomaty 2100xe USB, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú neautentifikovanému útočníkovi s fyzickým prístupom k zariadeniu získať neoprávnený prístup do systému a vykonať neoprávnené zmeny.

Dátum prvého zverejnenia varovania

20.08.2020

CVE

CVE-2020-9062

Zasiahnuté systémy

Diebold Nixdorf 2100xe USB verzia 1.1.30

Následky

Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Taktiež odporúčame zabezpečiť systém podľa odporúčaní výrobcu.

Zdroje

https://www.kb.cert.org/vuls/id/221785
https://exchange.xforce.ibmcloud.com/vulnerabilities/187015