BEZPEČNOSTNÝ BULLETIN

Týždeň 22. 06. 2022 - 28. 06. 2022

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Google Chrome - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
02.	Bosch PRA-ES8P2S - bezpečnostná zraniteľnosť	Vysoká	**8.8**
03.	MS SharePoint Server - bezpečnostná zraniteľnosť	Vysoká	**8.8**
04.	WatchGuard Firebox & XTM - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
05.	AtlasVPN - bezpečnostná zraniteľnosť	Vysoká	**8.5**
06.	Microsoft Edge - viacero bezpečnostných zraniteľností	Vysoká	**8.3**
07.	Open SSL - bezpečnostná zraniteľnosť	Stredná	**6.3**

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:
01794/2022/SK-CERT-803

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

Identifikátor

Google Chrome - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj internetový prehliadač Google Chrome, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webovej stránky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

21.06.2022

CVE

CVE-2022-2156, CVE-2022-2157, CVE-2022-2158, CVE-2022-2160, CVE-2022-2161, CVE-2022-2162, CVE-2022-2163, CVE-2022-2164, CVE-2022-2165

Zasiahnuté systémy

Google Chrome vo verzii staršej ako 103.0.5060.53

Následky

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

Odporúčania

Administrátorom a používateľom 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/2022/06/stable-channel-update-for-desktop_21.html
https://www.redpacketsecurity.com/google-chrome-base-code-execution-cve-2022-2156/
https://www.securityweek.com/google-patches-14-vulnerabilities-release-chrome-103

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

Identifikátor

Bosch PRA-ES8P2S - bezpečnostná zraniteľnosť

Popis

Spoločnosť Bosch vydala bezpečnostnú aktualizáciu na ethernetový switch PRA-ES8P2S, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom injekcie špeciálne vytvorených požiadaviek vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

22.06.2022

CVE

CVE-2022-32534, CVE-2022-32535, CVE-2022-32536

Zasiahnuté systémy

PRA-ES8P2S Ethernet-Switch vo verzii staršej ako 1.01.07

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Výrobca tiež odporúča zariadenie prevádzkovať izolované od internetu, vypnúť webové rozhranie a zariadenie konfigurovať pomocou konzoly.
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://psirt.bosch.com/security-advisories/BOSCH-SA-247052-BT.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/229550

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

Identifikátor

MS SharePoint Server - bezpečnostná zraniteľnosť

Popis

Spoločnosť Microsoft vydala bezpečnostnú aktualizáciu na svoj produkt Microsoft SharePoint Server, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

21.06.2022

CVE

CVE-2022-30157

Zasiahnuté systémy

Microsoft SharePoint Server vo verzii staršej ako KB5002224

Následky

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

Odporúčania

Administrátorom a používateľom 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://www.zerodayinitiative.com/advisories/ZDI-22-871/
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30157

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

Identifikátor

WatchGuard Firebox & XTM - viacero bezpečnostných zraniteľností

Popis

Spoločnosť WatchGuard Technologies vydala bezpečnostnú aktualizáciu na svoje firewally Firebox a XTM, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne upravených príkazov iniciovať update firmwéru zo škodlivého zdroja a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

23.06.2022

CVE

CVE-2022-25362, CVE-2022-31749, CVE-2022-31789, CVE-2022-31790, CVE-2022-31792

Zasiahnuté systémy

Fireware OS vo verzii staršej ako 12.8.1
Fireware OS 12.x vo verzii staršej ako 12.1.4
Fireware OS 12.2.x až 12.5.x vo verzii staršej ako 12.5.10

Následky

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

Odporúčania

Administrátorom a používateľom 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.ykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-watchguard-firebox-and-xtm-appliances-could-allow-for-remote-code-execution_2022-085
https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2022-00016

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.5
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

AtlasVPN - bezpečnostná zraniteľnosť

Popis

Vývojári VPN klienta AtlasVPN vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom špeciálne vytvoreného payloadu eskalovať svoje privilégiá a spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

20.06.2022

CVE

CVE-2022-23171

Zasiahnuté systémy

AtlasVPN vo verzii staršej ako 2.4.2

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému.

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom 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.redpacketsecurity.com/atlasvpn-privilege-escalation-cve-2022-23171/
https://www.gov.il/en/departments/faq/cve_advisories
https://www.securitynewspaper.com/2022/06/22/privilege-escalation-vulnerability-in-atlasvpn-update-immediately/

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

Identifikátor

Microsoft Edge - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Microsoft vydala bezpečnostnú aktualizáciu na svoj internetový prehliadač Microsoft Edge, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi
prostredníctvom podvrhnutia špeciálne vytvorenej webovej stránky eskalovať svoje privilégiá a spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

23.06.2022

CVE

CVE-2022-30192, CVE-2022-33638, CVE-2022-33639

Zasiahnuté systémy

Microsoft Edge vo verzii staršej ako 103.0.1264.37

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom 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://exchange.xforce.ibmcloud.com/vulnerabilities/229623
https://docs.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30192

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

Identifikátor

Open SSL - bezpečnostná zraniteľnosť

Popis

Vývojári toolkitu OpenSSL vydali bezpečnostnú aktualizáciu svojho produktu ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, nautentifikovanému útočníkovi s právomocami používateľa prostredníctvom injekcie špeciálne upravených príkazov získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

13.06.2022

CVE

CVE-2022-2068

Zasiahnuté systémy

OpenSSL vo verzii staršej ako 3.0.4
OpenSSL vo verzii staršej ako 1.1.1p
OpenSSL vo verzii staršej ako 1.0.2zf

Následky

Čiastočné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom 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://securityonline.info/cve-2022-2068-openssl-command-injection-vulnerability/
https://www.openssl.org/news/secadv/20220621.txt
https://vuldb.com/?id.202454