BEZPEČNOSTNÝ BULLETIN

Týždeň 25. 01. 2023 - 31. 01. 2023

OBSAH BEZPEČNOSTNÉHO BULLETINU

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-1019

BEZPEČNOSTNÝ BULLETIN

Týždeň 25. 01. 2023 - 31. 01. 2023

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 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

24.01.2023

CVE

CVE-2023-0471, CVE-2023-0472, CVE-2023-0473, CVE-2023-0474

Zasiahnuté systémy

Chrome Desktop
ChromeOS / ChromeOS Flex
Chrome 109 (109.0.5414.117/.118) for Android
Chrome Stable 109 (109.0.5414.112) for iOS

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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://chromereleases.googleblog.com/2023/01/stable-channel-update-for-desktop_24.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/245307

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-1019

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

Identifikátor

PowerDNS - bezpečnostná zraniteľnosť

Popis

Vývojári DNS rekurzora PowerDNS Recursor vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Kritická bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorených DNS dopytov spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

20.01.2023

CVE

CVE-2023-22617

Zasiahnuté systémy

PowerDNS Recursor vo verzii staršej ako 4.8.1

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.openwall.com/lists/oss-security/2023/01/20/1
https://www.redpacketsecurity.com/powerdns-recursor-denial-of-service-cve-2023-22617/
https://nvd.nist.gov/vuln/detail/CVE-2023-22617

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

Identifikátor

Delta Electronics CNCSoft - Bezpečnostná zraniteľnosť

Popis

Spoločnosť Delta Electronics vydala bezpečnostnú aktualizáciu na svoj produkt CNCSoft ScreenEditor, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

26.01.2023

CVE

CVE-2022-4634

Zasiahnuté systémy

Delta Electronics CNCSoft ScreenEditor vo verzii staršej ako 1.01.34

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace systémy a jednotky odporúčame prevádzkovať úplne oddelené od internetu.
Po odstránení zraniteľností, ktoré mohli spôsobiť vykonanie škodlivého kódu 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.cisa.gov/uscert/ics/advisories/icsa-23-026-01

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

Identifikátor

NVIDIA Jetson - bezpečnostná zraniteľnosť

Popis

Spoločnosť NVIDIA vydala bezpečnostné aktualizácie na produkty Jetson AGX Xavier Series, Jetson Xavier NX a Jetson AGX Orin Series, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom pretečenia zásobníka vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

25.01.2023

CVE

CVE-2022-42270

Zasiahnuté systémy

NVIDIA Jetson AGX Xavier Series, Jetson Xavier NX, Jetson AGX Orin Series vo verzii staršej ako 35.2.1 a 32.7.3

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.

Zdroje

https://nvidia.custhelp.com/app/answers/detail/a_id/5442

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

Identifikátor

Mitsubishi Electric MELFA SD/SQ a F-series Robot Controllers - Zraniteľnosti

Popis

Spoločnosť Mitsubishi Electric vydala bezpečnostné aktualizácie na svoje ovládače robotov MELFA SD/SQ a F-Series, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

26.01.2023

CVE

CVE-2022-33323

Zasiahnuté systémy

Mitsubishi Electric MELFA SD/SQ Series vo verzii staršej ako S7y
Mitsubishi Electric MELFA SD/SQ Series vo verzii staršej ako R7y
Mitsubishi Electric MELFA F-Series vo verzii staršej ako S7y
Mitsubishi Electric MELFA F-Series vo verzii staršej ako R7y

Následky

Neoprávnený prístup do systému

Odporúčania

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

Zdroje

https://www.cisa.gov/uscert/ics/advisories/icsa-23-026-05

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

Identifikátor

Junos OS pre vSRX Series - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Juniper Networks vydala bezpečnostnú aktualizáciu na svoj produkt Junos OS pre vSRX Series, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

11.01.2023

CVE

CVE-2023-22417

Zasiahnuté systémy

Junos OS pre vSRX Series vo verzii staršej ako 19.3R3-S7, 19.4R2-S8, 19.4R3-S10, 20.2R3-S6, 20.3R3-S5, 20.4R3-S5, 21.1R3-S4, 21.2R3, 21.3R3, 21.4R2, a 22.1R1

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Junos-OS-vSRX-Series-A-memory-leak-might-be-observed-in-IPsec-VPN-scenario-leading-to-an-FPC-crash-CVE-2023-22417?language=en_US

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

Identifikátor

BIND - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Internet Systems Consortium vydala bezpečnostné aktualizácie na svoj produkt Berkeley Internet Name Domain (BIND) 9, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom DNS flooding útoku spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

28.01.2023

CVE

CVE-2022-3094, CVE-2022-3488, CVE-2022-3736, CVE-2022-3924

Zasiahnuté systémy

BIND vo verzii staršej ako 9.16.37, 9.18.11, 9.19.9, a 9.16.37-S1

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://kb.isc.org/v1/docs/cve-2022-3094
https://thehackernews.com/2023/01/isc-releases-security-patches-for-new.html