BEZPEČNOSTNÝ BULLETIN

Týždeň 05. 07. 2023 - 11. 07. 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-1211

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

Identifikátor

TP-Link Tapo C210 - bezpečnostná zraniteľnosť

Popis

Spoločnosť TP-Link vydala bezpečnostnú aktualizáciu firmvéru na svoju IP kameru Tapo C210, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente zneužiť proces obnovenia hesla a získať neoprávnený prístup do systému a následne získať úplnú kontrolu nad systémom.

Dátum prvého zverejnenia varovania

05.07.2023

CVE

CVE-2023-35717

Zasiahnuté systémy

TP-Link Tapo C210 vo verzii firmvéru staršej ako 1.3.6 Build 230426 Rel.48373n

Následky

Neoprávnený prístup do systému
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://www.zerodayinitiative.com/advisories/ZDI-23-895/

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

Identifikátor

D-Link DAP-2622 - bezpečnostná zraniteľnosť

Popis

Spoločnosť D-Link vydala bezpečnostnú aktualizáciu na svoj WLAN prístupový bod DAP-2622, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente prostredníctvom pretečenia zásobníka vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

05.07.2023

CVE

CVE-2023-35718

Zasiahnuté systémy

D-Link DAP-2622 vo verzii firmvéru staršej ako v1.10B03 Beta-Hotfix

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://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10343
https://www.zerodayinitiative.com/advisories/ZDI-23-896/

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

Identifikátor

Apple Produkty - bezpečnostná zraniteľnosť

Popis

Spoločnosť Apple vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktoré opravujú bezpečnostnú zraniteľnosť.
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.
Zraniteľnosť je v súčasnosti aktívne zneužívaná útočníkmi.

Dátum prvého zverejnenia varovania

10.07.2023

CVE

CVE-2023-37450

Zasiahnuté systémy

macOS Ventura vo verzii staršej ako 13.4.1 (a)
iOS vo verzii staršej ako 16.5.1
iPadOS vo verzii staršej ako 16.5.1
Safari vo verzii staršej ako 16.5.2

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://support.apple.com/en-us/HT213826
https://support.apple.com/en-us/HT213823
https://support.apple.com/en-us/HT213825
https://www.macworld.com/article/1986514/rapid-security-response-ios-ipados-16-5-1-macos-13-4-1-update-webkit-zero-day.html

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

Identifikátor

Mozilla Produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Mozilla vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú 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

04.07.2023

CVE

CVE-2023-3482, CVE-2023-37201, CVE-2023-37202, CVE-2023-37203, CVE-2023-37204, CVE-2023-37205, CVE-2023-37206, CVE-2023-37207, CVE-2023-37208, CVE-2023-37209, CVE-2023-37210, CVE-2023-37211, CVE-2023-37212

Zasiahnuté systémy

Firefox ESR 102.13
Firefox 115
Thunderbird 102.13

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://www.mozilla.org/en-US/security/advisories/mfsa2023-24/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-22/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-23/

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

Identifikátor

SoftEther VPN - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Link vydala bezpečnostnú aktualizáciu na svoj produkt SoftEther VPN, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby alebo vykonanie škodlivého kódu s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

03.07.2023

CVE

CVE-2023-22325, CVE-2023-27395, CVE-2023-27516, CVE-2023-31192, CVE-2023-32275, CVE-2023-32634

Zasiahnuté systémy

SoftEther VPN vo verzii staršej ako 4.42 Build 9798 RTM

Následky

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

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://www.softether.org/9-about/News/904-SEVPN202301
http://jvn.jp/en/jp/JVN64316789/index.html

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

Identifikátor

Linux Kernel - dve bezpečnostné zraniteľnosti

Popis

Vývojári jadra operačného systému Linux vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

08.07.2023

CVE

CVE-2023-31248, CVE-2023-3269

Zasiahnuté systémy

Linux Kernel vo verzii staršej ako 6.1.37, 6.3.11 a 6.4.1

Následky

Eskalácia privilégií
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://access.redhat.com/security/cve/cve-2023-3269
https://github.com/lrh2000/StackRot
https://thehackernews.com/2023/07/researchers-uncover-new-linux-kernel.html
https://www.zerodayinitiative.com/advisories/ZDI-23-899/
https://github.com/advisories/GHSA-vr3g-637q-4rh6

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

Identifikátor

Canonical Ubuntu - bezpečnostná zraniteľnosť

Popis

Spoločnosť Canonical vydala bezpečnostnú aktualizáciu na svoju linuxovú distribúciu Ubuntu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

06.07.2023

CVE

CVE-2023-1829

Zasiahnuté systémy

Ubuntu pred commitom 8c710f75256bb3cf05ac7b1672c82b92c43f3d28

Následky

Eskalácia privilégií
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://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=8c710f75256bb3cf05ac7b1672c82b92c43f3d28
https://www.zerodayinitiative.com/advisories/ZDI-23-898/
https://nvd.nist.gov/vuln/detail/CVE-2023-1829

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

Identifikátor

Frauscher Diagnostic System FDS001 - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu Frauscher Diagnostic System FDS001.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

05.07.2023

CVE

CVE-2023-2880

Zasiahnuté systémy

Frauscher Diagnostic System FDS001 vo verzii staršej ako 1.3.3 (vrátane)

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Vzhľadom na to, že produkt už nie je udržiavaný, odporúčame prejsť na iný produkt s platnou podporou. Pre mitigáciu výrobca odporúča uistiť sa že k diagnostickému systému má prístup len oprávnený personál alebo osoby v jeho sprievode.

Zdroje

https://cert.vde.com/en/advisories/VDE-2023-011/

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

Identifikátor

IBM Db2 - viacero bezpečnostných zraniteľností

Popis

Spoločnosť IBM vydala bezpečnostné aktualizácie na svoj produkt IBM Db2, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

07.07.2023

CVE

CVE-2023-30443, CVE-2023-30445, CVE-2023-30446, CVE-2023-30447, CVE-2023-30448, CVE-2023-30449

Zasiahnuté systémy

IBM® Db2® vo verzii staršej ako 10.5.0.11 (vrátane)
IBM® Db2® vo verzii staršej ako 11.1.4.7 (vrátane)
IBM® Db2® vo verzii staršej ako 11.5.x (vrátane)

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkaze v časti ZDROJE

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.ibm.com/support/pages/node/7010557

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.4**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Cisco ACI - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti funkcionality ACI Multi-Site CloudSec šifrovania pre Cisco switche Nexus 9332C, 9364C a Cisco Nexus N9K-X9736C-FX Line Card.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom odpočúvania sieťovej prevádzky získať neoprávnený prístup k citlivým údajom a modifikovať obsah sieťovej komunikácie.

Dátum prvého zverejnenia varovania

05.07.2023

CVE

CVE-2023-20185

Zasiahnuté systémy

Cisco ACI vo všetkých verziách

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Vzhľadom na to, že produkt už nie je udržiavaný, odporúčame prejsť na iný produkt s platnou podporou.
Pre mitigáciu výrobca odporúča deaktivovať predmetnú funkcionalitu a kontaktovať ich zákaznícku podporu.

Zdroje

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.2
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Milesight UR32L - viacero bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach priemyselného routera Milesight UR32L.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom zaslania špeciálne vytvorenej HTTP požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

06.07.2023

CVE

CVE-2023-25081, CVE-2023-25082, CVE-2023-25083, CVE-2023-25084, CVE-2023-25085, CVE-2023-25086, CVE-2023-25087, CVE-2023-25088, CVE-2023-25089, CVE-2023-25090, CVE-2023-25091, CVE-2023-25092, CVE-2023-25093, CVE-2023-25094, CVE-2023-25095, CVE-2023-25096, CVE-2023-25097, CVE-2023-25098, CVE-2023-25099, CVE-2023-25100, CVE-2023-25101, CVE-2023-25102, CVE-2023-25103, CVE-2023-25104, CVE-2023-25105, CVE-2023-25106, CVE-2023-25107, CVE-2023-25108, CVE-2023-25109, CVE-2023-25110, CVE-2023-25111, CVE-2023-25112, CVE-2023-25113, CVE-2023-25114, CVE-2023-25115, CVE-2023-25116, CVE-2023-25117, CVE-2023-25118, CVE-2023-25119, CVE-2023-25120, CVE-2023-25121, CVE-2023-25122, CVE-2023-25123, CVE-2023-25124

Zasiahnuté systémy

Milesight UR32L vo verzii staršej ako v32.3.0.5 (vrátane)

Následky

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

Odporúčania

Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat 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.talosintelligence.com/vulnerability_reports/TALOS-2023-1716

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.2
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

ABUS TVIP - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti bezpečnostnej kamery TVIP od výrobcu ABUS.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom injekcie škodlivého skriptu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

06.07.2023

CVE

CVE-2023-26609

Zasiahnuté systémy

ABUS TVIP: 20000-21150 vo všetkých verziách firmvéru

Následky

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

Odporúčania

Vzhľadom na to, že produkt už nie je udržiavaný, odporúčame prejsť na iný produkt s platnou podporou.
Výrobca odporúča model TVIP82561.

Zdroje

https://www.cisa.gov/news-events/ics-advisories/icsa-23-187-02