BEZPEČNOSTNÝ BULLETIN

Týždeň 30. 08. 2023 - 05. 09. 2023

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Nvidia GeForce Now a DGX H100 - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
02.	Google Chrome - bezpečnostná zraniteľnosť	Vysoká	**8.8**
03.	PTC Codebeamer - bezpečnostná zraniteľnosť	Vysoká	**8.8**
04.	Mozilla produkty - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
05.	D-Link DAP-2622 - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
06.	NETGEAR Orbi 760 - bezpečnostná zraniteľnosť	Vysoká	**8.8**
07.	PaperCut NG - tri bezpečnostné zraniteľnosti	Vysoká	**8.8**
08.	Splunk Enterprise - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
09.	Acronis produkty - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
10.	Brocade SANnav a Fabric OS - viacero bezpečnostných zraniteľností	Vysoká	**8.6**
11.	RTS VLink Virtual Matrix Software - bezpečnostná zraniteľnosť	Vysoká	**8.4**
12.	All-in-One WP Migration rozšírenia - bezpečnostná zraniteľnosť	Vysoká	**7.3**
13.	TP-Link Tapo C210 - bezpečnostná zraniteľnosť	Vysoká	**7.2**
14.	IBM Financial Transaction Manager for SWIFT Services - bezpečnostná zraniteľnosť	Vysoká	**7.1**

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-1316

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

Identifikátor

Nvidia GeForce Now a DGX H100 - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Nvidia vydala bezpečnostné aktualizácie na svoje produkty GeForce Now a DGX H100, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente prostredníctvom zaslania špeciálne upravených paketov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

28.08.2023

CVE

CVE-2023-25527, CVE-2023-25528, CVE-2023-25529, CVE-2023-25530, CVE-2023-25531, CVE-2023-25532, CVE-2023-25533, CVE-2023-31008, CVE-2023-31009, CVE-2023-31010, CVE-2023-31011, CVE-2023-31012, CVE-2023-31013, CVE-2023-31014, CVE-2023-31015

Zasiahnuté systémy

DGX H100 BMC vo verziách starších ako 23.08.18
GeForce NOW pre Android mobile a TV app vo verzii staršej ako 6.05.33200069

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Zneprístupnenie služby
Neoprávnený prístup k citlivým údajom
Eskalácia privilégií

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/5473
https://nvidia.custhelp.com/app/answers/detail/a_id/5476

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

Identifikátor

Google Chrome - bezpečnostná zraniteľnosť

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

29.08.2023

CVE

CVE-2023-4572

Zasiahnuté systémy

Chrome pre Mac a Linux vo verzii staršej ako 116.0.5845.140
Chrome pre Windows vo verzii staršej ako 116.0.5845.140/.141

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/2023/08/stable-channel-update-for-desktop_29.html
https://stackdiary.com/rce-in-chrome-patched-cve-2023-4572/

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

Identifikátor

PTC Codebeamer - bezpečnostná zraniteľnosť

Popis

Spoločnosť PTC vydala bezpečnostnú aktualizáciu na svoj produkt Codebeamer, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom cross-site scripting (XSS) útoku vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Zneužitie zraniteľnosti vyžaduje interakciu používateľa.

Dátum prvého zverejnenia varovania

29.08.2023

CVE

CVE-2023-4296

Zasiahnuté systémy

PTC Codebeamer vo verzii staršej ako 22.10-SP8
PTC Codebeamer vo verzii staršej ako 22.04-SP6
PTC Codebeamer vo verzii staršej ako 21.09-SP14

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.cisa.gov/news-events/ics-advisories/icsa-23-241-01

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

29.08.2023

CVE

CVE-2023-4051, CVE-2023-4053, CVE-2023-4573, CVE-2023-4574, CVE-2023-4575, CVE-2023-4576, CVE-2023-4577, CVE-2023-4578, CVE-2023-4579, CVE-2023-4580, CVE-2023-4581, CVE-2023-4582, CVE-2023-4583, CVE-2023-4584, CVE-2023-4585

Zasiahnuté systémy

Thunderbird vo verzii staršej ako 102.15 a 115.2
Firefox ESR vo verzii staršej ako 102.15 a 115.2
Firefox vo verzii staršej ako 117

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/mfsa2023-38/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-34/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-35/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-36/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-37/

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

Identifikátor

D-Link DAP-2622 - viacero bezpečnostných zraniteľností

Popis

Spoločnosť D-Link vydala bezpečnostnú aktualizáciu na svoj produkt DAP-2622, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente prostredníctvom pretečenia zásobníka vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

25.08.2023

CVE

CVE-2023-35724, CVE-2023-35725, CVE-2023-35726, CVE-2023-35727, CVE-2023-35728, CVE-2023-35729, CVE-2023-35730, CVE-2023-35731, CVE-2023-35732, CVE-2023-35733, CVE-2023-35735, CVE-2023-35736, CVE-2023-35737, CVE-2023-35738, CVE-2023-35739, CVE-2023-35740, CVE-2023-35741, CVE-2023-35742, CVE-2023-35743, CVE-2023-35744, CVE-2023-35745, CVE-2023-35746, CVE-2023-35747, CVE-2023-35748, CVE-2023-35750, CVE-2023-35751, CVE-2023-35752, CVE-2023-35753, CVE-2023-35754, CVE-2023-35755, CVE-2023-35756, CVE-2023-35758, CVE-2023-37310, CVE-2023-37311, CVE-2023-37312, CVE-2023-37313, CVE-2023-37314, CVE-2023-37315, CVE-2023-37316, CVE-2023-37317, CVE-2023-37318, CVE-2023-37319, CVE-2023-37320, CVE-2023-37321, CVE-2023-37322, CVE-2023-37323, CVE-2023-37324, CVE-2023-37326

Zasiahnuté systémy

DAP-2622 vo verzii firmvéru staršej ako v1.10B03R022 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=SAP10349
https://www.zerodayinitiative.com/advisories/ZDI-23-1279/

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

Identifikátor

NETGEAR Orbi 760 - bezpečnostná zraniteľnosť

Popis

Spoločnosť NETGEAR vydala bezpečnostnú aktualizáciu na svoj router Orbi 760, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente obísť mechanizmy autentifikácie a získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

30.08.2023

CVE

CVE-2023-41183

Zasiahnuté systémy

RBR760 vo verzii firmvéru staršej ako 6.3.8.5

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 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://kb.netgear.com/000065734/Security-Advisory-for-Authentication-Bypass-on-the-RBR760-PSV-2023-0052
https://www.zerodayinitiative.com/advisories/ZDI-23-1283/

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

Identifikátor

PaperCut NG - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť PaperCut Software vydala bezpečnostnú aktualizáciu na svoj produkt PaperCut NG, ktorá opravuje tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom cross-site scripting (XSS) útoku vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

30.08.2023

CVE

CVE-2023-2533, CVE-2023-31046, CVE-2023-39469

Zasiahnuté systémy

PaperCut NG/MF vo verzii staršej ako 22.1.1

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://www.papercut.com/kb/Main/SecurityBulletinJune2023/
https://www.zerodayinitiative.com/advisories/ZDI-23-1285/

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

Identifikátor

Splunk Enterprise - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Splunk vydala bezpečnostnú aktualizáciu na svoj produkt Splunk Enterprise, 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 vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

30.08.2023

CVE

CVE-2023-40592, CVE-2023-40595, CVE-2023-40596, CVE-2023-40597, CVE-2023-40598, CVE-2023-4571

Zasiahnuté systémy

Splunk Enterprise vo verzii staršej ako 8.2.12, 9.0.6, a 9.1.1

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://advisory.splunk.com/advisories/SVD-2023-0804
https://www.securityweek.com/splunk-patches-high-severity-flaws-in-enterprise-it-service-intelligence/

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

Identifikátor

Acronis produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Acronis vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

31.08.2023

CVE

CVE-2022-46868, CVE-2022-46869, CVE-2023-41742, CVE-2023-41743, CVE-2023-41744, CVE-2023-41745, CVE-2023-41746, CVE-2023-41747, CVE-2023-41748, CVE-2023-41749, CVE-2023-41750, CVE-2023-41751, CVE-2023-4688

Zasiahnuté systémy

Acronis Cyber Protect Home Office (Windows) vo verzii staršej ako 40278
Acronis Agent (Windows) vo verzii staršej ako 31637
Acronis Cyber Protect 15 (Windows) vo verzii staršej ako 35979

Následky

Eskalácia privilégií
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://security-advisory.acronis.com/advisories/SEC-5487
https://security-advisory.acronis.com/updates/UPD-2304-c825-6d96
https://security-advisory.acronis.com/advisories/SEC-5382
https://security-advisory.acronis.com/advisories/SEC-4351
https://security-advisory.acronis.com/advisories/SEC-5287
https://security-advisory.acronis.com/advisories/SEC-5782
https://security-advisory.acronis.com/advisories/SEC-2008
https://security-advisory.acronis.com/advisories/SEC-5615
https://security-advisory.acronis.com/advisories/SEC-5811
https://security-advisory.acronis.com/advisories/SEC-2499
https://security-advisory.acronis.com/advisories/SEC-3835
https://security-advisory.acronis.com/advisories/SEC-4728
https://security-advisory.acronis.com/advisories/SEC-5810
https://security-advisory.acronis.com/advisories/SEC-5816

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.6
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Brocade SANnav a Fabric OS - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Broadcom vydala bezpečnostné aktualizácie na produkty Brocade SANnav a Fabric OS, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

29.08.2023

CVE

CVE-2015-1315, CVE-2016-1000027, CVE-2017-7657, CVE-2018-1273, CVE-2018-17190, CVE-2021-3711, CVE-2022-22950, CVE-2022-25647, CVE-2022-2625, CVE-2022-33980, CVE-2022-40664, CVE-2022-41946, CVE-2022-42889, CVE-2022-43937, CVE-2023-31423, CVE-2023-31424, CVE-2023-31925, CVE-2023-3489

Zasiahnuté systémy

Brocade SANnav vo verzii staršej ako v2.2.2a a v2.3.0
Brocade Fabric OS vo verzii staršej ako v9.2.0a

Následky

Neoprávnený prístup k citlivým údajom

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://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/22505
https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/22510

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.4
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

RTS VLink Virtual Matrix Software - bezpečnostná zraniteľnosť

Popis

Spoločnosť BOSCH vydala bezpečnostnú aktualizáciu na svoj produkt RTS VLink Virtual Matrix Software, ktorá opravuje bezpečnostnú zraniteľnosť.

Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom injekcie špeciálne upravených príkazov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

30.08.2023

CVE

CVE-2023-34999

Zasiahnuté systémy

RTS VLink Virtual Matrix vo verzii staršej ako 5.7.6
RTS VLink Virtual Matrix vo verzii staršej ako 6.5.0

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://psirt.bosch.com/security-advisories/bosch-sa-893251-bt.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.3
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

All-in-One WP Migration rozšírenia - bezpečnostná zraniteľnosť

Popis

Vývojári WordPress pluginu All-in-One WP Migration vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

30.08.2023

CVE

CVE-2023-40004

Zasiahnuté systémy

All-in-One WP Migration Box Extension 1.54
All-in-One WP Migration Google Drive Extension 2.80
All-in-One WP Migration OneDrive Extension 1.67
All-in-One WP Migration Dropbox Extension 3.76

Následky

Eskalácia privilégií
Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky založené na redakčnom systéme Wordpress nevyužívajú predmetné pluginy v zraniteľných verziách. V prípade, že áno, administrátorom odporúčame vykonať aktualizáciu zraniteľných 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://patchstack.com/articles/pre-auth-access-token-manipulation-in-all-in-one-wp-migration-extensions/
https://patchstack.com/database/vulnerability/all-in-one-wp-migration-box-extension/wordpress-all-in-one-wp-migration-box-extension-plugin-1-53-unauthenticated-access-token-manipulation-vulnerability

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

Identifikátor

TP-Link Tapo C210 - bezpečnostná zraniteľnosť

Popis

Spoločnosť TP-Link vydala bezpečnostnú aktualizáciu na svoju bezpečnostnú kameru, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

31.08.2023

CVE

CVE-2023-41184

Zasiahnuté systémy

Tapo C210 vo verzii staršej ako 1.3.6 Build 230426 Rel.48373n

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://exchange.xforce.ibmcloud.com/vulnerabilities/264889
https://www.zerodayinitiative.com/advisories/ZDI-23-1287/

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

Identifikátor

IBM Financial Transaction Manager for SWIFT Services - bezpečnostná zraniteľnosť

Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu na svoj produkt IBM Financial Transaction Manager for SWIFT Services, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvoreného XML dokumentu získať neoprávnený prístup k citlivým údajom a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

01.09.2023

CVE

CVE-2023-35892

Zasiahnuté systémy

IBM Financial Transaction Manager for SWIFT Services for Multiplatforms vo verzii staršej ako 3.2.4.10

Následky

Neoprávnený prístup k citlivým údajom
Zneprístupnenie služby

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.ibm.com/support/pages/node/7030359
https://exchange.xforce.ibmcloud.com/vulnerabilities/258786