BEZPEČNOSTNÝ BULLETIN

Týždeň 27. 09. 2023 - 03. 10. 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-1353

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

Identifikátor

D-Link DAR-8000 - dve bezpečnostné zraniteľnosti

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti routra DAR-8000.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.
Na uvedenú zraniteľnosť je v súčasnosti voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

25.09.2023

CVE

CVE-2023-5153, CVE-2023-5154

Zasiahnuté systémy

DAR-8000 vo verzii staršej ako 100a53dbr

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://cvepremium.circl.lu/cve/CVE-2023-5154
https://cvepremium.circl.lu/cve/CVE-2023-5153

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 Foundation vydala bezpečnostné aktualizácie na produkty Mozilla Firefox, Firefox ESR, Firefox Focus pre Android, Firefox pre Android a Thunderbird, 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

26.09.2023

CVE

CVE-2023-5168, CVE-2023-5169, CVE-2023-5170, CVE-2023-5171, CVE-2023-5172, CVE-2023-5173, CVE-2023-5174, CVE-2023-5175, CVE-2023-5176

Zasiahnuté systémy

Firefox 118.0.1
Firefox ESR 115.3.1
Firefox Focus for Android 118.1
Firefox for Android 118.1
Thunderbird 115.3

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.

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/mfsa2023-44/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-43/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-41/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-42/
https://exchange.xforce.ibmcloud.com/vulnerabilities/266999

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

Identifikátor

Google Chrome - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Google vydala bezpečnostné aktualizácie na internetové prehliadače Chrome, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webstránky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

28.09.2023

CVE

CVE-2023-5186, CVE-2023-5187, CVE-2023-5217

Zasiahnuté systémy

Chrome vo verzii staršej ako 116.0.5845.228

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/2023/09/stable-channel-update-for-desktop_27.html
https://chromereleases.googleblog.com/2023/09/chrome-for-android-update_0480966349.html

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

Identifikátor

Gstreamer - tri bezpečnostné zraniteľnosti

Popis

Vývojári platformy Gstreamer vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

27.09.2023

CVE

CVE-2023-40474, CVE-2023-40475, CVE-2023-40476

Zasiahnuté systémy

GStreamer vo verzii staršej ako 1.22.6

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://gstreamer.freedesktop.org/security/sa-2023-0008.html
https://www.zerodayinitiative.com/advisories/ZDI-23-1456/
https://www.zerodayinitiative.com/advisories/ZDI-23-1457/
https://www.zerodayinitiative.com/advisories/ZDI-23-1458/

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

Identifikátor

Os Commerce - viacero bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktu Os Commerce.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom XSS (Cross Site Scripting) útoku vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

29.09.2023

CVE

CVE-2023-43702, CVE-2023-43703, CVE-2023-43704, CVE-2023-43705, CVE-2023-43706, CVE-2023-43707, CVE-2023-43708, CVE-2023-43709, CVE-2023-43710, CVE-2023-43711, CVE-2023-43712, CVE-2023-43713, CVE-2023-43714, CVE-2023-43715, CVE-2023-43716, CVE-2023-43717, CVE-2023-43718, CVE-2023-43719, CVE-2023-43720, CVE-2023-43721, CVE-2023-43722, CVE-2023-43723, CVE-2023-43724, CVE-2023-43725, CVE-2023-43726, CVE-2023-43727, CVE-2023-43728, CVE-2023-43729, CVE-2023-43730, CVE-2023-43731, CVE-2023-43732, CVE-2023-43733, CVE-2023-43734, CVE-2023-43735, CVE-2023-43736, CVE-2023-5111, CVE-2023-5112

Zasiahnuté systémy

Os Commerce vo verzii staršej ako 4.12.56860 (vrátane)

Následky

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

Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú frameworky, knižnice, pluginy, SDK alebo moduly v zraniteľnej verzii. V prípade, že áno, odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat zabezpečiť aktualizáciu všetkých komponentov, od ktorých závisí vaša aplikácia, na aktuálne verzie bez známych bezpečnostných zraniteľností.
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://fluidattacks.com/advisories/bts/

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

Identifikátor

Openfire - bezpečnostná zraniteľnosť

Popis

Vývojári RTC servera Openfire vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

23.05.2023

CVE

CVE-2023-32315

Zasiahnuté systémy

Openfire vo verzii staršej ako 4.6.8, 4.7.5, a 4.8.0

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://nvd.nist.gov/vuln/detail/CVE-2023-32315
https://www.bleepingcomputer.com/news/security/hackers-actively-exploiting-openfire-flaw-to-encrypt-servers

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

Identifikátor

Safari a macOS Sonoma 14 - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Apple vydala bezpečnostné aktualizácie na produkty Safari a macOS Sonoma, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

28.09.2023

CVE

CVE-2023-23495, CVE-2023-29497, CVE-2023-32361, CVE-2023-32377, CVE-2023-32396, CVE-2023-32421, CVE-2023-35074, CVE-2023-35984, CVE-2023-35990, CVE-2023-37448, CVE-2023-38586, CVE-2023-38596, CVE-2023-38615, CVE-2023-39233, CVE-2023-39434, CVE-2023-40384, CVE-2023-40386, CVE-2023-40388, CVE-2023-40391, CVE-2023-40395, CVE-2023-40399, CVE-2023-40400, CVE-2023-40402, CVE-2023-40403, CVE-2023-40406, CVE-2023-40407, CVE-2023-40410, CVE-2023-40417, CVE-2023-40420, CVE-2023-40422, CVE-2023-40424, CVE-2023-40426, CVE-2023-40427, CVE-2023-40429, CVE-2023-40432, CVE-2023-40434, CVE-2023-40436, CVE-2023-40441, CVE-2023-40448, CVE-2023-40450, CVE-2023-40451, CVE-2023-40452, CVE-2023-40454, CVE-2023-40455, CVE-2023-40541, CVE-2023-41063, CVE-2023-41065, CVE-2023-41066, CVE-2023-41067, CVE-2023-41070, CVE-2023-41073, CVE-2023-41074, CVE-2023-41078, CVE-2023-41079, CVE-2023-41968, CVE-2023-41979, CVE-2023-41980, CVE-2023-41981, CVE-2023-41984, CVE-2023-41986, CVE-2023-41993, CVE-2023-41995

Zasiahnuté systémy

Safari 17
macOS Sonoma 14

Následky

Vykonanie škodlivého kódu
Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.apple.com/en-us/HT213941
https://support.apple.com/en-us/HT213940

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.0**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Advantech EKI-1524-CE - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Advantech vydala bezpečnostnú aktualizáciu na svoje produkty EKI-1524-CE, EKI-1522-CE a EKI-1521-CE, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom XSS (Cross Site Scripting) útoku vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

26.09.2023

CVE

CVE-2023-4202, CVE-2023-4203

Zasiahnuté systémy

EKI-1524/ EKI-1524-CE/ EKI-1524CI-CE vo verzii firmvéru staršej ako EKI-1524-CE_D1.26_r6775_994E1244
EKI-1522/ EKI-1522-CE/ EKI-1522CI-CE vo verzii firmvéru staršej ako EKI-1522-CE_D1.26_r6775_9959FFFE
EKI-1521/ EKI-1521-CE/ EKI-1521CI-CE vo verzii firmvéru staršej ako EKI-1521-CE_D1.26_r6775_997DB607

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-23-269-04

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.0**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

DEXMA DEXGate - viacero bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktu DEXGate.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente prostredníctvom XSS (Cross Site Scripting) útoku získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

28.09.2023

CVE

CVE-2023-40153, CVE-2023-4108, CVE-2023-41088, CVE-2023-42435, CVE-2023-42666

Zasiahnuté systémy

DEXGate vo všetkých verziách

Následky

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.
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.cisa.gov/news-events/ics-advisories/icsa-23-271-02
https://support.dexma.com/hc/en-gb/articles/360007865414-DEXGate-Full-Documentation

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

Identifikátor

Chrome OS/Chrome OS Flex - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj operačný systém Chrome OS/Chrome OS Flex, ktorá opravuje 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

26.09.2023

CVE

CVE-2023-4208, CVE-2023-4622, CVE-2023-4863, CVE-2023-4900, CVE-2023-4901, CVE-2023-4902, CVE-2023-4903, CVE-2023-4904, CVE-2023-4905, CVE-2023-4906, CVE-2023-4907, CVE-2023-4908, CVE-2023-4909

Zasiahnuté systémy

Chrome OS vo verzii staršej ako 15572.50.0

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://chromereleases.googleblog.com/2023/09/stable-channel-update-for-chromeos.html

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

Identifikátor

Avast Premium Security - dve zero-day bezpečnostné zraniteľnosti

Popis

Bezpečnostní výskumníci zverejnili informácie o zero-day zraniteľnostiach produktu Avast Premium Security.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom podvrhnutia špeciálne vytvoreného symbolického odkazu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

27.09.2023

CVE

CVE-2023-42123, CVE-2023-42124

Zasiahnuté systémy

Avast Premium Security vo verzii staršej ako 23.9.8494.0 (vrátane)

Následky

Eskalácia privilégií
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.zerodayinitiative.com/advisories/ZDI-23-1475/
https://www.zerodayinitiative.com/advisories/ZDI-23-1474/

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

Identifikátor

Dell Common Event Enabler - bezpečnostná zraniteľnosť

Popis

Spoločnosť Dell vydala bezpečnostnú aktualizáciu na svoj produkt Common Event Enabler, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť znepristupnenie služby.

Dátum prvého zverejnenia varovania

29.09.2023

CVE

CVE-2023-32477

Zasiahnuté systémy

Dell CEE vo verzii staršej ako 8.9.9.0

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://www.dell.com/support/kbdoc/en-us/000218120/dsa-2023-310-security-update-for-dell-emc-common-event-enabler
https://exchange.xforce.ibmcloud.com/vulnerabilities/267347

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

Identifikátor

Bently Nevada 3500 System - tri bezpečnostné zraniteľnosti

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktu Bently Nevada 3500. Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

26.09.2023

CVE

CVE-2023-34437, CVE-2023-34441, CVE-2023-36857

Zasiahnuté systémy

Bently Nevada 3500 Rack vo verzii TDI firmvéru staršej ako 5.05

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Na uvedené zraniteľnosti v súčasnosti nie sú dostupné aktualizácie. Odporúčame postupovať podľa odporúčaní od výrobcu, ktoré môžete nájsť na webovej adrese v časti ZDROJE.
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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN). Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.

Zdroje

https://www.cisa.gov/news-events/ics-advisories/icsa-23-269-05
https://dam.bakerhughes.com/media/?mediaId=32F7FC2F-9F22-4C69-BB847565B7834D08

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.9
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Hitachi Energy Asset Suite 9 - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu Asset Suite 9.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora vykonať neoprávnené zmeny v systéme a zneprístupnenie služby.

Dátum prvého zverejnenia varovania

26.09.2023

CVE

CVE-2023-4816

Zasiahnuté systémy

Asset Suite vo verzii staršej ako 9.6.4 (vrátane)
Asset Suite vo verzii staršej ako 9.6.3.11.1 (vrátane)

Následky

Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné aktualizácie. Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov. Do vydania záplat odporúčame postupovať podľa odporúčaní výrobcu, ktoré môžete nájsť na webovej adrese v časti ZDROJE.

Zdroje

https://www.cisa.gov/news-events/ics-advisories/icsa-23-269-02
https://images.go.hitachienergy.com/Web/ABBEnterpriseSoftware/%7B70b3d323-4866-42e1-8a75-58996729c1d4%7D_8DBD000172-VU-2023-23_Asset_Suite_Tagout_vulnerability_Rev1.pdf

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

Identifikátor

VMware Aria Operations - bezpečnostná zraniteľnosť

Popis

Spoločnosť VMware vydala bezpečnostné aktualizácie na produkty Aria Operations, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami administrátora eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

26.09.2023

CVE

CVE-2023-34043

Zasiahnuté systémy

VMware Aria Operations vo verzii staršej ako 8.12 Hot Fix 5
VMware Aria Operations vo verzii staršej ako 8.10 Hot Fix 9
VMware Aria Operations vo verzii staršej ako 8.6 Hot Fix 11
VMware Cloud Foundation (VMware Aria Operations) vo verzii staršej ako KB92148
VMware Cloud Foundation (VMware Aria Operations) vo verzii staršej ako KB92148

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://www.vmware.com/security/advisories/VMSA-2023-0020.html

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

Identifikátor

Suprema BioStar 2 - bezpečnostná zraniteľnosť

Popis

Spoločnosť Suprema vydala bezpečnostnú aktualizáciu na svoj produkt BioStar 2, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom SQL injekcie získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

26.09.2023

CVE

CVE-2023-27167

Zasiahnuté systémy

BioStar 2 2.9.4

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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN). Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.

Zdroje

https://www.cisa.gov/news-events/ics-advisories/icsa-23-269-01