BEZPEČNOSTNÝ BULLETIN

Týždeň 24. 05. 2023 - 30. 05. 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-1167

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

Identifikátor

HPE Aruba EdgeConnect Enterprise - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Hewlett Packard vydala bezpečnostné aktualizácie na svoj produkt Aruba EdgeConnect Enterprise, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom injekcie špeciálne upravených príkazov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

24.05.2023

CVE

CVE-2023-30501, CVE-2023-30502, CVE-2023-30503, CVE-2023-30504, CVE-2023-30505, CVE-2023-30506, CVE-2023-30507, CVE-2023-30508, CVE-2023-30509, CVE-2023-30510

Zasiahnuté systémy

Aruba EdgeConnect Enterprise ECOS vo verzii staršej ako 9.3.0.0
Aruba EdgeConnect Enterprise ECOS vo verzii staršej ako 9.2.4.0
Aruba EdgeConnect Enterprise ECOS vo verzii staršej ako 9.1.6.0
Aruba EdgeConnect Enterprise ECOS vo verzii staršej ako 9.0.9.0

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://nvd.nist.gov/vuln/detail/CVE-2023-30501
https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04480en_us

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

Identifikátor

Hitachi Energy AFS65x, AFS67x, AFR67x a AFF66x - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Hitachi Energy vydala bezpečnostné aktualizácie na produkty AFS67x, AFR67x a AFF66x, ktoré opravujú dve bezpečnostné zraniteľnosti.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom znovupoužitia uvoľnenej pamäte získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

23.05.2023

CVE

CVE-2022-40674, CVE-2022-43680

Zasiahnuté systémy

AFS660/665S, AFS660/665C, AFS670v2 vo verzii firmvéru staršej ako 7.1.08
AFS670/675, AFR67x vo verzii firmvéru staršej ako 9.1.08
AFF660/665 vo verzii firmvéru staršej ako 03.0.02 (vrátane)
AFS65x vo všetkých verziách firmvéru (End of life)

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. Pri produktoch, pre ktoré ešte neboli vydané bezpečnostné záplaty, odporúčame zraniteľnosti mitigovať podľa odporúčaní od výrobcu, sledovať stránky výrobcu a po vydaní príslušných záplat systémy aktualizovať. Pre produkty, ktoré už nie sú udržiavané 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-23-143-01

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

Identifikátor

Horner Automation - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Horner Automation vydala bezpečnostnú aktualizáciu na svoje produkty Cscape a Cscape Envision RV, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

23.05.2023

CVE

CVE-2023-27916, CVE-2023-28653, CVE-2023-29503, CVE-2023-31244, CVE-2023-31278, CVE-2023-32203, CVE-2023-32281, CVE-2023-32289, CVE-2023-32539, CVE-2023-32545

Zasiahnuté systémy

Cscape vo verzii staršej ako v9.90 SP9
Cscape Envision RV vo verzii staršej ako v4.80

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.cisa.gov/news-events/ics-advisories/icsa-23-143-04

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

Identifikátor

iTunes - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Apple vydala bezpečnostnú aktualizáciu na svoj produkt iTunes for Windows, ktorá opravuje dve bezpečnostné zraniteľnosti.
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

23.05.2023

CVE

CVE-2023-32351, CVE-2023-32353

Zasiahnuté systémy

iTunes pre Windows vo verzii staršej ako 12.12.9

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://support.apple.com/en-us/HT213763
https://www.redpacketsecurity.com/apple-itunes-for-windows-privilege-escalation-cve-2023-32351/

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

Identifikátor

Autodesk - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Autodesk vydala bezpečnostnú aktualizáciu na svoj produkt Autodesk® Installer, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom podvrhnutia špeciálne vytvorených DLL súborov eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

23.04.2023

CVE

CVE-2023-27906, CVE-2023-27908

Zasiahnuté systémy

Autodesk® Installer vo verzii staršej ako 1.39.0.216

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
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://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0010
https://www.zerodayinitiative.com/advisories/ZDI-23-712/

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

Identifikátor

Adobe produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom pretečenia zásobníka vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

25.05.2023

CVE

CVE-2022-24101, CVE-2022-24102, CVE-2022-24103, CVE-2022-24104, CVE-2022-27785, CVE-2022-27786, CVE-2022-27787, CVE-2022-27788, CVE-2022-27789, CVE-2022-27790, CVE-2022-27791, CVE-2022-27792, CVE-2022-27793, CVE-2022-27794, CVE-2022-27795, CVE-2022-27796, CVE-2022-27797, CVE-2022-27798, CVE-2022-27799, CVE-2022-27800, CVE-2022-27801, CVE-2022-27802, CVE-2022-28230, CVE-2022-28231, CVE-2022-28232, CVE-2022-28233, CVE-2022-28234, CVE-2022-28235, CVE-2022-28236, CVE-2022-28237, CVE-2022-28238, CVE-2022-28239, CVE-2022-28240, CVE-2022-28241, CVE-2022-28242, CVE-2022-28243, CVE-2022-28244, CVE-2022-28245, CVE-2022-28246, CVE-2022-28247, CVE-2022-28248, CVE-2022-28249, CVE-2022-28250, CVE-2022-28251, CVE-2022-28252, CVE-2022-28253, CVE-2022-28254, CVE-2022-28255, CVE-2022-28256, CVE-2022-28257, CVE-2022-28258, CVE-2022-28259, CVE-2022-28260, CVE-2022-28261, CVE-2022-28262, CVE-2022-28263, CVE-2022-28264, CVE-2022-28265, CVE-2022-28266, CVE-2022-28267, CVE-2022-28268, CVE-2022-28269, CVE-2022-28837, CVE-2022-28838, CVE-2022-35672, CVE-2022-44512, CVE-2022-44513, CVE-2022-44514, CVE-2022-44515, CVE-2022-44516, CVE-2022-44517, CVE-2022-44518, CVE-2022-44519, CVE-2022-44520, CVE-2023-21601, CVE-2023-21603

Zasiahnuté systémy

Acrobat DC vo verzii staršej ako 22.001.20117 (Win)
Acrobat DC vo verzii staršej ako 22.001.20112 (Mac)
Acrobat Reader DC vo verzii staršej ako 22.001.20117 (Win)
Acrobat Reader DC vo verzii staršej ako 22.001.20112 (Mac)
Acrobat 2020 vo verzii staršej ako 20.005.30334 (Win)
Acrobat 2020 vo verzii staršej ako 20.005.30331 (Mac)
Acrobat Reader 2020 vo verzii staršej ako 20.005.30334 (Win)
Acrobat Reader 2020 vo verzii staršej ako 20.005.30331 (Mac)
Acrobat 2017 vo verzii staršej ako 17.012.30229 (Win)
Acrobat 2017 vo verzii staršej ako 17.012.30227 (Mac)
Acrobat Reader 2017 vo verzii staršej ako 17.012.30229 (Win)
Acrobat Reader 2017 vo verzii staršej ako 17.012.30227 (Mac)

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://helpx.adobe.com/security/products/acrobat/apsb22-16.html

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

Identifikátor

Wacom Driver - dve zero-day bezpečnostné zraniteľnosti

Popis

Bezpečnostní výskumníci zverejnili informácie o zero-day zraniteľnostiach driverov pre zariadenia značky Wacom.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom podvrhnutia špeciálne vytvorených súborov eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Na uvedenú zraniteľnosť je v súčasnosti voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

26.05.2023

CVE

CVE-2023-32162, CVE-2023-32163

Zasiahnuté systémy

Wacom Driver for Windows vo všetkých verziách

Následky

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

Odporúčania

Na uvedené zraniteľnosti v súčasnosti nie sú dostupné aktualizácie. 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-23-741/
https://www.zerodayinitiative.com/advisories/ZDI-23-742/

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

Identifikátor

LibreOffice - bezpečnostná zraniteľnosť

Popis

Vývojári softvérového balíka LibreOffice vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

28.05.2023

CVE

CVE-2023-0950

Zasiahnuté systémy

LibreOffice 7.4 vo verzii staršej ako 7.4.6
LibreOffice 7.5 vo verzii staršej ako 7.5.1.

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

Zdroje

https://www.redpacketsecurity.com/libreoffice-code-execution-cve-2023-0950/

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

Identifikátor

Prestashop Customexporter - bezpečnostná zraniteľnosť

Popis

Vývojári modulu Customexporter pre plugin Prestashop vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.
Zraniteľnosť je v súčasnosti aktívne zneužívaná útočníkmi.

Dátum prvého zverejnenia varovania

19.05.2023

CVE

CVE-2023-30199

Zasiahnuté systémy

Prestashop Customexporter vo verzii staršej ako 1.7.21

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://friends-of-presta.github.io/security-advisories/modules/2023/05/16/customexporter.html
https://nvd.nist.gov/vuln/detail/CVE-2023-30199
https://www.redpacketsecurity.com/prestashop-customexporter-information-disclosure-cve-2023-30199/

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

Identifikátor

Mikrotik RouterOS - bezpečnostná zraniteľnosť

Popis

Spoločnosť Mikrotik vydala bezpečnostnú aktualizáciu na svoj produkt RouterOS, ktorá opravuje bezpečnostnú zraniteľnosť.
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

10.05.2023

CVE

CVE-2023-32154

Zasiahnuté systémy

MikroTik RouterOS vo verzii staršej ako 7.9

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.zerodayinitiative.com/advisories/ZDI-23-710/

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.1
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

TrendMicro Apex Central - viacero bezpečnostných zraniteľností

Popis

Spoločnosť TrendMicro vydala bezpečnostnú aktualizáciu na svoj produkt Apex Central, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom SQL injekcie vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

24.05.2023

CVE

CVE-2023-32529, CVE-2023-32531, CVE-2023-32536, CVE-2023-32537, CVE-2023-32604, CVE-2023-32605

Zasiahnuté systémy

Apex Central vo verzii staršej ako Patch 4 (B6394)

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://success.trendmicro.com/dcx/s/solution/000293107?language=en_US
https://www.zerodayinitiative.com/advisories/ZDI-23-726/
https://www.zerodayinitiative.com/advisories/ZDI-23-725/
https://www.zerodayinitiative.com/advisories/ZDI-23-724/
https://www.zerodayinitiative.com/advisories/ZDI-23-723/