BEZPEČNOSTNÝ BULLETIN

Týždeň 19. 04. 2023 - 25. 04. 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-1108

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

Identifikátor

Woocommerce Email Report WP Plugin - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti WordPress pluginu Woocommerce Email Report.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať XSS útok (Cross Site Scripting).

Dátum prvého zverejnenia varovania

21.04.2023

CVE

CVE-2023-27627

Zasiahnuté systémy

Woocommerce Email Report vo verzii staršej ako 2.4

Následky

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

Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú predmetný framework zraniteľnej verzii. V prípade, že áno, odporúčame plugin dočasne deaktivovať, sledovať stránky výrobcu a po vydaní príslušných záplat systémy aktualizovať.
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://patchstack.com/database/vulnerability/wooemailreport/wordpress-woocommerce-email-report-plugin-2-4-cross-site-scripting-xss-vulnerability

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

Identifikátor

SolarWinds - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť SolarWinds vydala bezpečnostnú aktualizáciu na svoj produkt SolarWinds Platform, ktorá opravuje tri bezpečnostné zraniteľnosti.
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

18.04.2023

CVE

CVE-2022-36963, CVE-2022-47505, CVE-2022-47509

Zasiahnuté systémy

SolarWinds Platform vo verzii staršej ako 2023.2

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. V prípade, že aktualizácia systému nie je možná, výrobca odporúča zneprístupniť platformu SolarWinds z verejného internetu, znefunkčniť nepotrebné porty, protokoly a služby na Vašom hostujúcom operačnom systéme a aplikáciách ako SQL Server, zabezpečenie riadnej segmentácie siete, a od Orion Platform 2020.2.1 Hotfix 2 vyššie (vrátane) je možné nastaviť spúšťanie akcii upozornení Solar Platform výlučne na kontext limitovaného používateľského konta.
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.solarwinds.com/trust-center/security-advisories/cve-2022-36963
https://www.securityweek.com/solarwinds-platform-update-patches-high-severity-vulnerabilities/

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

Identifikátor

Ivanti Avalanche - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Ivanti vydala bezpečnostnú aktualizáciu na svoj produkt Avalanche, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa obísť mechanizmus autentifikácie a získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

24.04.2023

CVE

CVE-2023-28125, CVE-2023-28126, CVE-2023-28127, CVE-2023-28128

Zasiahnuté systémy

Ivanti Avalanche vo verzii staršej ako 6.4

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://www.zerodayinitiative.com/advisories/ZDI-23-456/
https://www.zerodayinitiative.com/advisories/ZDI-23-455/
https://www.zerodayinitiative.com/advisories/ZDI-23-454/
https://www.zerodayinitiative.com/advisories/ZDI-23-453/

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

Identifikátor

NVIDIA Produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť NVIDIA vydala bezpečnostné aktualizácie na servery DGX-1, NVIDIA CUDA Toolkit a firmware ConnectX, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť nachádzajúca sa v NVIDIA DGX-1 SBIOS spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami administrátora eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

19.04.2023

CVE

CVE-2020-12357, CVE-2020-12358, CVE-2020-12359, CVE-2020-12360, CVE-2020-24486, CVE-2020-8670, CVE-2020-8700, CVE-2021-0095, CVE-2023-0203, CVE-2023-0204, CVE-2023-0205, CVE-2023-0209, CVE-2023-25510, CVE-2023-25511, CVE-2023-25512, CVE-2023-25513, CVE-2023-25514

Zasiahnuté systémy

NVIDIA DGX-1 Servery s BMC vo verzii staršej ako 3.39.3 alebo s SBIOS vo verzii staršej ako S2W_3A13
NVIDIA ConnectX Firmware vo verzii staršej ako 35.1012
NVIDIA CUDA Toolkit vo verzii staršej ako 12.1 Update 1

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Bezpečnostná záplata je obsiahnutá v aktualizácii UEFI BIOS, preto používateľom odporúčame nainštalovať aktualizácie systému UEFI BIOS z webových stránok výrobcu pre ich konkrétne elektronické zariadenie. V prípade, že prevádzkujete fyzické servery s operačným systémom Linux, uistite sa, že máte nainštalovaný balík intel-microcode. Na BSD systémoch môžete použiť balík cpupdate.
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/5458
https://nvidia.custhelp.com/app/answers/detail/a_id/5459
https://nvidia.custhelp.com/app/answers/detail/a_id/5456

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

Identifikátor

Linux Kernel - bezpečnostná zraniteľnosť

Popis

Vývojári jadra operačného systému Linux vydali bezpečnostnú aktualizáciu svojho produktu, 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

19.04.2023

CVE

CVE-2023-2124

Zasiahnuté systémy

Linux Debian 10 vo verzii staršej ako 4.19.249-2 (vrátane)
Linux Debian 11 vo verzii staršej ako 5.10.158-2 (vrátane)
Linux Debian 12 vo verzii staršej ako 6.1.20-2 (vrátane)

Následky

Eskalácia privilégií
Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Pri produktoch, pre ktoré ešte neboli vydané bezpečnostné záplaty, odporúčame zraniteľnosti mitigovať podľa odporúčaní od vývojárov, sledovať stránky výrobcu a po vydaní príslušných záplat systémy aktualizovať.
Detailné inštrukcie môžete nájsť na webovej adrese https://lore.kernel.org/linux-xfs/20230412214034.GL3223426@dread.disaster.area/t/#mb15f4ba9d4be6f0fcee3dd7f3b1fcc7cb2f652a6.
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://exchange.xforce.ibmcloud.com/vulnerabilities/253226
https://seclists.org/oss-sec/2023/q2/62
https://avd.aliyun.com/detail?id=AVD-2023-2124

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

Identifikátor

OMRON CX-Drive & SYSMAC CS/CJ Series - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť OMRON vydala bezpečnostné aktualizácie na produkty CX-Drive & SYSMAC CS/CJ Series, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v produkte CX-Drive, 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

24.04.2023

CVE

CVE-2022-45794, CVE-2023-27385

Zasiahnuté systémy

CX-Drive vo verzii staršej ako 3.01 (vrátane)
SYSMAC CJ2H-CPU6[]-EIP vo všetkých verziách
SYSMAC CJ2H-CPU6[] vo všetkých verziách
SYSMAC CJ2M-CPU[][] vo všetkých verziách
SYSMAC CJ1G-CPU[][]P vo všetkých verziách
SYSMAC CS1H-CPU[][]H vo všetkých verziách
SYSMAC CS1G-CPU[][]H vo všetkých verziách
SYSMAC CS1D-CPU[][]HA vo všetkých verziách
SYSMAC CS1D-CPU[][]H vo všetkých verziách
SYSMAC CS1D-CPU[][]SA vo všetkých verziách
SYSMAC CS1D-CPU[][]S vo všetkých verziách
SYSMAC CS1D-CPU[][]P vo všetkých verziách

Následky

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

Odporúčania

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.
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.
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.ia.omron.com/product/vulnerability/OMSR-2023-004_en.pdf
https://www.cisa.gov/news-events/ics-advisories/icsa-23-108-01

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

Identifikátor

Drupal - bezpečnostná zraniteľnosť

Popis

Vývojári redakčného systému Drupal 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.

Dátum prvého zverejnenia varovania

19.04.2023

CVE

-

Zasiahnuté systémy

Drupal vo verzii staršej ako 10.0.8.
Drupal vo verzii staršej ako 9.5.8.
Drupal vo verzii staršej ako 9.4.14.
Drupal vo verzii staršej ako 7.96.
Drupal 8 vo všetkých verziách (EoL)

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://www.drupal.org/sa-core-2023-005

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

Identifikátor

VMware Tanzu Spring Boot - bezpečnostná zraniteľnosť

Popis

Spoločnosť VMware vydala bezpečnostné aktualizácie na svoj produkt Tanzu Spring Boot, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

20.04.2023

CVE

CVE-2023-20873

Zasiahnuté systémy

Spring Boot vo verzii staršej ako 3.0.6
Spring Boot vo verzii staršej ako 2.7.11

Následky

Neoprávnená zmena v systéme

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://spring.io/security/cve-2023-20873
https://exchange.xforce.ibmcloud.com/vulnerabilities/253466

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

Identifikátor

Dell Display Manager - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Dell vydala bezpečnostnú aktualizáciu na svoj produkt Dell Display Manager, 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 súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

20.04.2023

CVE

CVE-2023-28046, CVE-2023-28047

Zasiahnuté systémy

Dell Display Manager vo verzii staršej ako 2.1.1

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.dell.com/support/kbdoc/sk-sk/000211727/dsa-2023