# BEZPEČNOSTNÝ BULLETIN

Týždeň 13. 03. 2024 - 19. 03. 2024

## 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**
Web: https://www.sk-cert.sk

# BEZPEČNOSTNÝ BULLETIN

Týždeň 13. 03. 2024 - 19. 03. 2024

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

## Identifikátor

Apple GarageBand - bezpečnostná zraniteľnosť

## Popis

Spoločnosť Apple vydala bezpečnostnú aktualizáciu na svoj produkt GarageBand, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-23300 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného súboru vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Zneužitie zraniteľnosti vyžaduje interakciu používateľa.

## Dátum prvého zverejnenia varovania

12.3.2024

## CVE

CVE-2024-23300

## Zasiahnuté systémy

GarageBand pre macOS Ventura a macOS Sonoma vo verzii staršej ako 10.4.11

## Následky

Vykonanie škodlivého kódu
Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
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.
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/HT214090
https://www.tenable.com/cve/CVE-2024-23300

| | | | | | |
|---|---|---|---|---|---|
| **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 bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-2400 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. Zneužitie zraniteľnosti vyžaduje interakciu používateľa.

## Dátum prvého zverejnenia varovania

12.3.2024

## CVE

CVE-2024-2400

## Zasiahnuté systémy

Google Chrome pre Windows a Mac vo verzii staršej ako 122.0.6261.128/.129
Google Chrome pre Linux vo verzii staršej ako 122.0.6261.128 (bezpečnostná záplata bude dostupná v nasledovných dňoch/ týždňoch)

## Následky

Vykonanie škodlivého kódu
Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

## Zdroje

https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_12.html
https://www.tenable.com/cve/CVE-2024-2400

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

## Identifikátor

LabVIEW - viacero bezpečnostných zraniteľností

## Popis

Spoločnosť NI vydala bezpečnostnú aktualizáciu na svoj produkt LabVIEW, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti s identifikátormi CVE-2024-23611, CVE-2024-23610, CVE-2024-23608, CVE-2024-23609, CVE-2024-23609 a CVE-2024-23612 spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených VI súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

12.3.2024

## CVE

CVE-2024-23609,CVE-2024-23608,CVE-2024-23610,CVE-2024-23611,CVE-2024-23612,CVE-2024-23609

## Zasiahnuté systémy

LabVIEW 2024 vo verzii staršej ako Q1 Patch 1

## Následky

Vykonanie škodlivého kódu
Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

## Zdroje

https://www.zerodayinitiative.com/advisories/ZDI-24-285/
https://www.zerodayinitiative.com/advisories/ZDI-24-286/
https://www.zerodayinitiative.com/advisories/ZDI-24-287/
https://www.zerodayinitiative.com/advisories/ZDI-24-288/
https://www.zerodayinitiative.com/advisories/ZDI-24-289/
https://www.zerodayinitiative.com/advisories/ZDI-24-290/
https://www.ni.com/en/support/security/available-critical-and-security-updates-for-ni-software/out-of-bounds-write-due-to-missing-bounds-check-in-labview.html
https://www.ni.com/en/support/security/available-critical-and-security-updates-for-ni-software/improper-error-handling-issues-in-labview.html

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

## Identifikátor

Delta Electronics DIAEnergie - viacero bezpečnostných zraniteľností

## Popis

Spoločnosť Delta Electronics vydala bezpečnostnú aktualizáciu na svoj produkt DIAEnergie, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2024-28029 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, 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.
Ostatné bezpečnostné zraniteľnosti možno zneužiť na vykonanie škodlivého kódu, neoprávnený prístup k citlivým údajom, neoprávnené zmeny v systéme a zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

14.3.2024

## CVE

CVE-2024-28029, CVE-2024-28891, CVE-2024-25937, CVE-2024-28040, CVE-2024-23975, CVE-2024-23494, CVE-2024-25574, CVE-2024-28171, CVE-2024-25567, CVE-2024-28045

## Zasiahnuté systémy

DIAEnergie vo verzii staršej ako v1.10.00.005

## Následky

Eskalácia privilégií
Vykonanie škodlivého kódu
Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Zneprístupnenie služby

## Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. Bezpečnostná aktualizácia je dostupná na vlastnú žiadosť od výrobcu prostredníctvom formulára dostupného na odkaze uvedenom v sekcii ZDROJE.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom alebo vzdialené vykonanie kódu, 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-24-074-12
https://www.deltaww.com/en/customerService

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

## Identifikátor

RegistrationMagic WP plugin - bezpečnostná zraniteľnosť

## Popis

Vývojári RegistrationMagic pluginu pre WordPress vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-1991 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, 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

14.3.2024

## CVE

CVE-2024-1991

## Zasiahnuté systémy

RegistrationMagic WP plugin vo verzii staršej ako 5.3.1.0

## Následky

Eskalácia privilégií
Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Zneprístupnenie služby

## Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú frameworky, knižnice, pluginy, SDK alebo moduly v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu všetkých komponentov, od ktorých závisí vaša aplikácia, na aktuálne verzie bez známych bezpečnostných zraniteľností.
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/database/vulnerability/custom-registration-form-builder-with-submission-manager/wordpress-registrationmagic-plugin-5-3-0-0-authenticated-subscriber-privilege-escalation-vulnerability
https://wordpress.org/plugins/custom-registration-form-builder-with-submission-manager/

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

## Identifikátor

Sciener TTLock aplikácia - viacero bezpečnostných zraniteľností

## Popis

Bezpečnostní výskumníci zverejnili informácie o viacerých zraniteľnostiach smart zámku Sciener TTLock.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2023-7017 spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňujú útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente prostredníctvom zaslania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

7.3.2024

## CVE

CVE-2023-7006, CVE-2023-7005, CVE-2023-7003, CVE-2023-6960, CVE-2023-7004, CVE-2023-7007, CVE-2023-7009, CVE-2023-7017

## Zasiahnuté systémy

Kontrol Lux lock vo verziách firmvéru od 6.5. do 6.5.07
Gateway G2 vo verzii firmvéru 6.0.0
TTLock App vo verzii 6.4.5

## Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Zneprístupnenie služby

## Odporúčania

Vzhľadom na absenciu záplat pre predmetné zraniteľnosti odporúčame administrátorom sledovať stránku výrobcu a po vydaní bezpečnostných záplat bezodkladne vykonať aktualizáciu zasiahnutých systémov.
Pred zneužitím zraniteľnosti sa možno chrániť deaktiváciou funkcionalít spojených s Bluetooth v Sciener firmvéri. Nakoľko elektronické zámky boli navrhnuté tak, aby sa ovládali pomocou aplikácie TTLock, deaktiváciou týchto funkcionalít sa však znemožní ich ovládanie na diaľku.
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.kb.cert.org/vuls/id/949046
https://alephsecurity.com/2024/02/20/kontrol-lux-lock-1/
https://alephsecurity.com/2024/03/07/kontrol-lux-lock-2/
https://exchange.xforce.ibmcloud.com/vulnerabilities/285093
https://www.securityweek.com/unpatched-sceiner-smart-lock-vulnerabilities-allow-hackers-to-open-doors/

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

## Identifikátor

Ashlar-Vellum Cobalt - bezpečnostná zraniteľnosť

## Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktu Cobalt.
Bezpečnostné zraniteľnosti spočívajú v nedostatočnom overovaní používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnuitia špeciálne vytvorených STP súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Zneužitie zraniteľnosti vyžaduje interakciu zo strany používateľa.

## Dátum prvého zverejnenia varovania

5.3.2024

## CVE

## Zasiahnuté systémy

Ashlar-Vellum Cobalt vo všetkých verziách

## Následky

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

## Odporúčania

Vzhľadom na absenciu záplat pre predmetné zraniteľnosti odporúčame administrátorom sledovať stránku výrobcu a po vydaní bezpečnostných záplat bezodkladne vykonať aktualizáciu zasiahnutých systémov.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
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-24-234/
https://www.zerodayinitiative.com/advisories/ZDI-24-235/
https://www.zerodayinitiative.com/advisories/ZDI-24-236/
https://www.zerodayinitiative.com/advisories/ZDI-24-237/
https://www.zerodayinitiative.com/advisories/ZDI-24-238/
https://www.zerodayinitiative.com/advisories/ZDI-24-239/
https://www.zerodayinitiative.com/advisories/ZDI-24-240/
https://www.zerodayinitiative.com/advisories/ZDI-24-241/
https://www.zerodayinitiative.com/advisories/ZDI-24-242/
https://www.zerodayinitiative.com/advisories/ZDI-24-243/
https://www.zerodayinitiative.com/advisories/ZDI-24-244/
https://www.zerodayinitiative.com/advisories/ZDI-24-245/
https://www.zerodayinitiative.com/advisories/ZDI-24-246/
https://www.zerodayinitiative.com/advisories/ZDI-24-247/
https://www.zerodayinitiative.com/advisories/ZDI-24-248/
https://www.zerodayinitiative.com/advisories/ZDI-24-249/
https://www.cybersecurity-help.cz/vdb/SB2024030624

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

## Identifikátor

Hustle WP plugin - bezpečnostná zraniteľnosť

## Popis

Vývojári WordPress pluginu Hustle vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-0368 spočíva v umiestnení API kľúčov priamo do zdrojového kódu a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

## Dátum prvého zverejnenia varovania

12.3.2024

## CVE

CVE-2024-0368

## Zasiahnuté systémy

Hustle WP plugin vo verzii staršej ako 7.8.4

## Následky

Neoprávnený prístup k citlivým údajom

## Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky a aplikácie založené na redakčnom systéme WordPress nevyužívajú predmetný plugin v zraniteľnej verzii. V prípade, že áno, bezodkladne zabezpečte aktualizáciu redakčného systému a všetkých používaných pluginov na aktuálne verzie bez známych bezpečnostných zraniteľností.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom alebo vzdialené vykonanie kódu, 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.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/wordpress-popup/hustle-783-sensitive-information-exposure-via-exposed-hubspot-api-keys

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

## Identifikátor

IBM i - bezpečnostná zraniteľnosť

## Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu na svoj produkt IBM i, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-22346 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov umožňuje lokálnemu, 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

13.3.2024

## CVE

CVE-2024-22346

## Zasiahnuté systémy

IBM i vo verzii 7.5, 7.4, 7.3 a 7.2 bez aplikovanej dočasnej PTF bezpečnostnej záplaty

Presnú špecifikáciu jednotlivých zasiahnutých produktov a konkrétnych PTF bezpečnostných záplat nájdete na webovej adrese:
https://www.ibm.com/support/pages/node/7140499

## Následky

Eskalácia privilégií
Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
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://exchange.xforce.ibmcloud.com/vulnerabilities/280203
https://www.ibm.com/support/pages/node/7140499
https://nvd.nist.gov/vuln/detail/CVE-2024-22346

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

## Identifikátor

HPE Unified OSS Console - viacero bezpečnostných zraniteľností

## Popis

Spoločnosť Hewlett Packard Enterprise (HPE) vydala bezpečnostnú aktualizáciu na svoj produkt HPE Unified OSS Console, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2024-22243 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom SSRF (server-side request forgery) útoku získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme. Zneužitie zraniteľnosti vyžaduje interakciu používateľa.
Zneužitím ostatných bezpečnostných zraniteľností možno vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

15.3.2024

## CVE

CVE-2022-34169, CVE-2023-5072, CVE-2022-45688, CVE-2024-25710, CVE-2024-26308, CVE-2024-22243

## Zasiahnuté systémy

HPE Unified OSS Console Assurance Monitoring (UOCAM) vo verzii staršej ako v3.1.3

## Následky

Vykonanie škodlivého kódu
Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

## Zdroje

https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04618en_us
https://nvd.nist.gov/vuln/detail/CVE-2024-22243

# BEZPEČNOSTNÝ BULLETIN

Týždeň 13. 03. 2024 - 19. 03. 2024

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

## Identifikátor

Ubuntu PostgreSQL a Open vSwitch - tri bezpečnostné zraniteľnosti

## Popis

Vývojári Linux distribúcie Ubuntu vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2024-0985 sa nachádza v produkte PostgreSQL, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom podvrhnutia špeciálne upravených príkazov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Zneužitie zraniteľnosti vyžaduje interakciu používateľa, ktorý vykoná podvrhnuté príkazy.
Zneužitím ostatných bezpečnostných zraniteľností možno spôsobiť zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

12.3.2024

## CVE

CVE-2023-3966, CVE-2023-5366, CVE-2024-0985

## Zasiahnuté systémy

PostgreSQL:
Ubuntu 16.04 s postgresql-9.5 vo verzii staršej ako 9.5.25-0ubuntu0.16.04.1+esm7 dostupné pre Ubuntu Pro
Ubuntu 16.04 s postgresql-client-9.5 vo verzii staršej ako 9.5.25-0ubuntu0.16.04.1+esm7 dostupné pre Ubuntu Pro
Po aplikovaní záplaty, pre vykonanie nevyhnutných zmien, výrobca odporúča reštart PostgreSQL.

Open vSwitch:
Ubuntu 23.10 s openvswitch-common vo verzii staršej ako 3.2.2-0ubuntu0.23.10.1
Ubuntu 23.10 s python3-openvswitch vo verzii staršej ako 3.2.2-0ubuntu0.23.10.1
Ubuntu 22.04 s openvswitch-common vo verzii staršej ako 2.17.9-0ubuntu0.22.04.1
Ubuntu 22.04 s python3-openvswitch vo verzii staršej ako 2.17.9-0ubuntu0.22.04.1
Ubuntu 20.04 s openvswitch-common vo verzii staršej ako 2.13.8-0ubuntu1.4
Ubuntu 20.04 s python3-openvswitch vo verzii staršej ako 2.13.8-0ubuntu1.4

## Následky

Vykonanie škodlivého kódu
Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
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://ubuntu.com/security/notices/USN-6690-1
https://www.auscert.org.au/bulletins/ESB-2024.1554/
https://ubuntu.com/security/notices/USN-6656-2
https://www.auscert.org.au/bulletins/ESB-2024.1557/

**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**
Web: https://www.sk-cert.sk

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

## Identifikátor

Dell iDRAC8 - bezpečnostná zraniteľnosť

## Popis

Spoločnosť Dell vydala bezpečnostnú aktualizáciu na svoj produkt iDRAC8, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť identifikátorom CVE-2024-25951 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje autentifikovanému útočníkovi s právomocami používateľa, ktorý sa nachádza v rovnakom sieťovom segmente prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

8.3.2024

## CVE

CVE-2024-25951

## Zasiahnuté systémy

iDRAC8 vo verzii staršej ako 2.85.85.85

## Následky

Vykonanie škodlivého kódu
Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
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://exchange.xforce.ibmcloud.com/vulnerabilities/285240
https://www.dell.com/support/kbdoc/en-us/000222591/dsa-2024-089-security-update-for-dell-idrac8-local-racadm-vulnerability

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

## Identifikátor

Tenable Nessus Agent - bezpečnostná zraniteľnosť

## Popis

Spoločnosť Tenable vydala bezpečnostné aktualizácie na produkty Nessus a Nessus Agent, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-2390 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby. Zneužitie zraniteľnosti vyžaduje interakciu používateľa.

## Dátum prvého zverejnenia varovania

14.3.2024

## CVE

CVE-2024-2390

## Zasiahnuté systémy

Tenable Plugin pre Nessus vo verzii staršej ako #202403142053
Tenable Plugin pre Nessus Agent vo verzii staršej ako #202403142053

## Následky

Eskalácia privilégií
Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

## Zdroje

https://www.tenable.com/security/tns-2024-05
https://www.auscert.org.au/bulletins/ESB-2024.1635/

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

## Identifikátor

Intel produkty - viacero bezpečnostných zraniteľností

## Popis

Spoločnosť Intel vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2023-32666 sa nachádza v procesoroch 4th Generation Intel® Xeon®, 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 a vykonať neoprávnené zmeny v systéme.
Zneužitím ostatných bezpečnostných zraniteľností možno eskalovať svoje privilégiá, získať neoprávnený prístup k citlivým údajom a spôsobiť zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

12.3.2024

## CVE

CVE-2023-32666, CVE-2023-32282, CVE-2023-32633, CVE-2023-28389, CVE-2023-35191, CVE-2023-28746, CVE-2023-22655, CVE-2023-39368, , CVE-2023-38575, CVE-2023-43490

## Zasiahnuté systémy

10th Generation Intel® Core™ Processor Family
11th Generation Intel® Core Processor Family
12th Generation Intel® Core™ Processor Family
3rd Gen Intel® Xeon® Scalable Processor Family
4th Generation Intel® Xeon® Bronze processors
4th Generation Intel® Xeon® Gold processors
4th Generation Intel® Xeon® Gold Processors
4th Generation Intel® Xeon® Platinum processors
4th Generation Intel® Xeon® Scalable processors
4th Generation Intel® Xeon® Silver processors
Intel® Atom®: x6211E, x6413E, x6425E, x6212RE, x6414RE, x6425RE, x6427FE, x6200FE
Intel® Celeron® Processor Family
Intel® Celeron®: J6413, N6211.
Intel® Core®:i7-11700T, i7-11700, i5-11400T, i5-11400, i5-11500T, i5-11500
Intel® CSME software
Intel® Local Manageability Service
Intel® Pentium® Gold Processor Family
Intel® Pentium®: J6425, N6415.
Intel® SPS
Intel® Xeon® CPU Max Series processors
Intel® Xeon® D Processor
Intel® Xeon® D Processor
Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkazoch v sekcii ZDROJE

Ďalšie špecifikácie jednotlivých zasiahnutých produktov nájdete na webovej adrese:
https://www.intel.com/content/www/us/en/developer/topic-technology/software-security-guidance/processors-affected-consolidated-product-cpu-model.html

## Následky

Eskalácia privilégií
Neoprávnený prístup k citlivým údajom

Neoprávnená zmena v systéme
Zneprístupnenie služby

## Odporúčania

Administrátorom a používateľom odporúčame bezodkladne 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.
SK-CERT administrátorom odporúča venovať osobitnú pozornosť aktualizácii firmvéru, nie len aplikačnému softvéru.

## Zdroje

https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00986.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00929.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00923.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00898.html
https://www.intel.com/content/www/us/en/developer/topic-technology/software-security-guidance/processors-affected-consolidated-product-cpu-model.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00960.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00972.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00982.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01045.html