# BEZPEČNOSTNÝ BULLETIN

Týždeň 11. 10. 2023 - 17. 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-1370

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

## Identifikátor

Chrome - viacero bezpečnostných zraniteľností

## Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj webový prehliadač Google Chrome, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webovej stránky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

10.10.2023

## CVE

CVE-2023-5218, CVE-2023-5473, CVE-2023-5474, CVE-2023-5475, CVE-2023-5476, CVE-2023-5477, CVE-2023-5478, CVE-2023-5479, CVE-2023-5481, CVE-2023-5483, CVE-2023-5484, CVE-2023-5485, CVE-2023-5486, CVE-2023-5487

## Zasiahnuté systémy

Google Chrome pre Mac a Linux vo verzii staršej ako 118.0.5993.70
Google Chrome pre Windows vo verzii staršej ako 118.0.5993.70/.71

## 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/2023/10/stable-channel-update-for-desktop_10.html

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

## Identifikátor

libcue/GNOME - bezpečnostná zraniteľnosť

## Popis

Vývojári balíka libcue vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených CUE súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Zneužitie zraniteľnosti vyžaduje interakciu používateľov.

## Dátum prvého zverejnenia varovania

10.10.2023

## CVE

CVE-2023-43641

## Zasiahnuté systémy

libcue vo verzii staršej ako 2.3.0

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

## Zdroje

https://thehackernews.com/2023/10/libcue-library-flaw-opens-gnome-linux.html
https://github.com/lipnitsk/libcue/security/advisories/GHSA-5982-x7hv-r9cj
https://nvd.nist.gov/vuln/detail/CVE-2023-43641

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

## Identifikátor

SAP produkty - viacero bezpečnostných zraniteľností

## Popis

Spoločnosť SAP vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktorá opravuje viacero bezpečnostných zraniteľností.
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

09.10.2023

## CVE

CVE-2023-31405, CVE-2023-40310, CVE-2023-41365, CVE-2023-42473, CVE-2023-42474, CVE-2023-42475, CVE-2023-42477

## Zasiahnuté systémy

SAP Business Client
SAP BusinessObjects Web Intelligence
SAP PowerDesigner Client
SAP NetWeaver AS Java
S/4HANA
SAP Business One

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkaze v časti ZDROJE.

## 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.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html
https://nvd.nist.gov/vuln/detail/CVE-2023-42474

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

## Identifikátor

Google Android - viacero bezpečnostných zraniteľností

## Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj open-source operačný systém Android, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov 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

02.10.2023

## CVE

CVE-2021-44828, CVE-2022-28348, CVE-2023-20819, CVE-2023-21244, CVE-2023-21252, CVE-2023-21253, CVE-2023-21266, CVE-2023-21291, CVE-2023-21673, CVE-2023-22385, CVE-2023-24843, CVE-2023-24844, CVE-2023-24847, CVE-2023-24848, CVE-2023-24849, CVE-2023-24850, CVE-2023-24853, CVE-2023-24855, CVE-2023-28540, CVE-2023-32819, CVE-2023-32820, CVE-2023-33026, CVE-2023-33027, CVE-2023-33028, CVE-2023-33029, CVE-2023-33034, CVE-2023-33035, CVE-2023-33200, CVE-2023-34970, CVE-2023-40116, CVE-2023-40117, CVE-2023-40120, CVE-2023-40121, CVE-2023-40123, CVE-2023-40125, CVE-2023-40127, CVE-2023-40128, CVE-2023-40129, CVE-2023-40130, CVE-2023-40131, CVE-2023-40133, CVE-2023-40134, CVE-2023-40135, CVE-2023-40136, CVE-2023-40137, CVE-2023-40138, CVE-2023-40139, CVE-2023-40140, CVE-2023-40638, CVE-2023-4211, CVE-2023-4863

## Zasiahnuté systémy

Google Android s bezpečnostnou aktualizáciou spred 1. Októbra 2023

## 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://source.android.com/docs/security/bulletin/2023-10-01

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☐ **Stredná** | ☒ **Vysoká** | ☐ **Kritická** | **CVSS skóre:** 8.8 |
| **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 nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

10.10.2023

## CVE

CVE-2023-26366, CVE-2023-26367, CVE-2023-26368, CVE-2023-26370, CVE-2023-38216, CVE-2023-38217, CVE-2023-38218, CVE-2023-38219, CVE-2023-38220, CVE-2023-38221, CVE-2023-38249, CVE-2023-38250, CVE-2023-38251

## Zasiahnuté systémy

Adobe Commerce vo verzii staršej ako 2.4.7-beta2 pre 2.4.7-beta1
Adobe Commerce vo verzii staršej ako 2.4.6-p3 pre 2.4.6-p2
Adobe Commerce vo verzii staršej ako 2.4.5-p5 pre 2.4.5-p4
Adobe Commerce vo verzii staršej ako 2.4.4-p6 pre 2.4.4-p5
Adobe Commerce vo verzii staršej ako 2.4.3-ext-5 pre 2.4.3-ext-4
Adobe Commerce vo verzii staršej ako 2.4.2-ext-5 pre 2.4.2-ext-4
Adobe Commerce vo verzii staršej ako 2.4.1-ext-5 pre 2.4.1-ext-4
Adobe Commerce vo verzii staršej ako 2.4.0-ext-5 pre 2.4.0-ext-4
Adobe Commerce vo verzii staršej ako 2.3.7-p4-ext-5 pre 2.3.7-p4-ext-4
Magento Open Source vo verzii staršej ako 2.4.7-beta2 pre 2.4.7-beta1
Magento Open Source vo verzii staršej ako 2.4.6-p3 pre 2.4.6-p2
Magento Open Source vo verzii staršej ako 2.4.5-p5 pre 2.4.5-p4
Magento Open Source vo verzii staršej ako 2.4.4-p6 pre 2.4.4-p5
Adobe Bridge vo verzii staršej ako 13.0.4
Adobe Bridge vo verzii staršej ako 14.0.1
Photoshop 2023 vo verzii staršej ako 24.7.1
Photoshop 2024 vo verzii staršej ako 25

## Následky

Eskalácia privilégií
Úplné narušenie dôvernosti, integrity a dostupnosti systému

| **Odporúčania** |
| --- |
| Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.<br>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://helpx.adobe.com/security/products/photoshop/apsb23-51.html<br>https://helpx.adobe.com/security/products/bridge/apsb23-49.html<br>https://helpx.adobe.com/security/products/magento/apsb23-50.html |

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

## Identifikátor

Apple produkty - dve bezpečnostné zraniteľnosti

## Popis

Spoločnosť Apple vydala bezpečnostné aktualizácie na operačné systémy iOS a iPadOS, ktoré opravujú dve bezpečnostné zraniteľnosti.

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

04.10.2023

## CVE

CVE-2023-42824, CVE-2023-5217

## Zasiahnuté systémy

iOS vo verzii staršej ako 17.0.3
iPadOS vo verzii staršej ako 17.0.3

## 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://support.apple.com/en-us/HT213961
https://support.apple.com/en-us/HT213972

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

## Identifikátor

ER2000 edge routers - viacero bezpečnostných zraniteľností

## Popis

Spoločnosť ConnectedIO vydala bezpečnostnú aktualizáciu na svoje portfólio routrov ER2000, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne upravených príkazov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

03.10.2023

## CVE

CVE-2023-33372, CVE-2023-33373, CVE-2023-33374, CVE-2023-33375, CVE-2023-33376, CVE-2023-33377, CVE-2023-33378, CVE-2023-33379

## Zasiahnuté systémy

ConnectedIO vo verzii staršej ako v2.1.0 (vrátane)

## 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://claroty.com/team82/research/the-path-to-the-cloud-is-filled-with-holes-exploiting-4g-edge-routers

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

## Identifikátor

libcurl - bezpečnostná zraniteľnosť

## Popis

Vývojári knižnice libcurl vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom pretečenia zásobníka 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

11.10.2023

## CVE

CVE-2023-38545, CVE-2023-38546

## Zasiahnuté systémy

libcurl vo verzii staršej ako 8.4.0

## Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
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 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://curl.se/docs/CVE-2023-38545.html<br>https://socradar.io/curl-update-available-for-cve-2023-38545-and-cve-2023-38546-high-severity-vulnerability-could-lead-to-rce/<br>https://daniel.haxx.se/blog/2023/10/11/curl-8-4-0/<br>https://www.synopsys.com/blogs/software-security/critical-libcurl-curl-vulnerabilities.html<br>https://jfrog.com/blog/curl-libcurl-october-2023-vulns-all-you-need-to-know/<br>https://www.apollographql.com/blog/graphql/security/apollos-response-to-cve-2023-38545/<br>https://github.com/curl/curl/discussions/12026<br>https://twitter.com/_JohnHammond/status/1711913166165463220<br>https://www.helpnetsecurity.com/2023/10/10/curl-vulnerabilities-cve-2023-38545/<br>https://isc.sans.edu/diary/CVE202338545+curl+SOCKS5+oversized+hostname+vulnerability+How+bad+is+it/30304 |

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

## Identifikátor

Mitsubishi Electric MELSEC-Q series PLCs - bezpečnostná zraniteľnosť

## Popis

Spoločnosť Mitsubishi Electric vydala bezpečnostnú aktualizáciu na svoje programovateľné logické radiče série MELSEC-Q, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne upravených paketov spôsobiť zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

10.10.2023

## CVE

CVE-2019-6535

## Zasiahnuté systémy

Q03/04/06/13/26UDVCPU staršie ako so sériovým číslom 20081 (vrátane)
Q04/06/13/26UDPVCPU staršie ako so sériovým číslom 20081 (vrátane)
Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU staršie ako so sériovým číslom 20101 (vrátane)

## Následky

Zneprístupnenie služby

## Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
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-19-029-02

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☐ **Stredná** | ☒ **Vysoká** | ☐ **Kritická** | **CVSS skóre:** 7.4 |
| **Klasifikácia** | ☒ **Neutajované / TLP(CLEAR)** | | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

FortiOS a FortiProxy - viacero bezpečnostných zraniteľností

## Popis

Spoločnosť Fortinet vydala bezpečnostné aktualizácie na produkty FortiOS a FortiProxy, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a vykonať neoprávnené zmeny v systéme a zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

10.10.2023

## CVE

CVE-2023-33301, CVE-2023-36555, CVE-2023-37935, CVE-2023-41675, CVE-2023-41841

## Zasiahnuté systémy

FortiOS 7.4 vo verzii staršej ako 7.4.0
FortiOS 7.2 vo verzii staršej ako 7.2.5
FortiOS 7.0 vo verzii staršej ako 7.0.12
FortiProxy vo verzii staršej ako 7.2.3
FortiProxy vo verzii staršej ako 7.0.9

## Následky

Eskalácia privilégií
Neoprávnená zmena v systéme
Zneprístupnenie služby

## Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

## Zdroje

https://www.fortiguard.com/psirt/FG-IR-23-318
https://www.fortiguard.com/psirt/FG-IR-23-184
https://www.fortiguard.com/psirt/FG-IR-23-104
https://www.fortiguard.com/psirt/FG-IR-23-120
https://www.fortiguard.com/psirt/FG-IR-23-139

**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-1370