# BEZPEČNOSTNÝ BULLETIN

Týždeň 22. 02. 2023 - 28. 02. 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-1056

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

## Identifikátor

Google Chrome - viacero bezpečnostných zraniteľností

## Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj internetový prehliadač 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

22.02.2023

## CVE

CVE-2023-0927, CVE-2023-0928, CVE-2023-0929, CVE-2023-0930, CVE-2023-0931, CVE-2023-0932, CVE-2023-0933, CVE-2023-0941

## Zasiahnuté systémy

Chrome pre Windows vo verzii staršej ako 110.0.5481.177/.178
Chrome pre Mac a Linux vo verzii staršej ako 110.0.5481.177

## 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/2023/02/stable-channel-desktop-update_22.html
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-chrome-could-allow-for-arbitrary-code-execution_2023-024

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

## Identifikátor

HPE produkty - viacero bezpečnostných zraniteľností

## Popis

Spoločnosť Hewlett Packard Enterprise vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v produkte Serviceguard, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

21.02.2023

## CVE

CVE-2022-36348, CVE-2022-37936, CVE-2022-37937, CVE-2022-37938

## Zasiahnuté systémy

HPE Serviceguard pre Linux vo verzii staršej ako A.12.80.05 a A.15.00.00
HPE Synergy 480 Gen10 Plus Compute Module s firmvérom vo verzii staršej ako 04.04.04.300
HPE StoreEasy 1660 Storage s firmvérom vo verzii staršej ako 04.04.04.300 (U46 ROM Family)
HPE StoreEasy 1860 Storage s firmvérom vo verzii staršej ako 04.04.04.300 (U46 ROM Family)
HPE ProLiant DX360 Gen10 Plus server s firmvérom vo verzii staršej ako 04.04.04.300
HPE ProLiant DX380 Gen10 Plus server s firmvérom vo verzii staršej ako 04.04.04.300

## 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://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbmu04452en_us
https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04420en_us
https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04429en_us
https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04435en_us

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

## Identifikátor

Apple macOS, iOS, iPadOS - dve bezpečnostné zraniteľnosti

## Popis

Spoločnosť Apple vydala bezpečnostné aktualizácie na produkty macOS Ventura, iOS a iPadOS, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

20.02.2023

## CVE

CVE-2023-23520, CVE-2023-23530

## Zasiahnuté systémy

macOS Ventura vo verzii staršej ako 13.2
iOS vo verzii staršej ako 16.3
iPadOS vo verzii staršej ako 16.3

## 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.

## Zdroje

https://www.trellix.com/en-us/about/newsroom/stories/research/trellix-advanced-research-center-discovers-a-new-privilege-escalation-bug-class-on-macos-and-ios.html
https://support.apple.com/en-us/HT213605
https://support.apple.com/en-us/HT213606
https://www.redpacketsecurity.com/apple-ios-ipados-and-macos-ventura-information-disclosure-cve-2023-23520-4/
https://www.redpacketsecurity.com/apple-ios-ipados-and-macos-ventura-privilege-escalation-cve-2023-23530-4/

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

## Identifikátor

Aruba produkty - viacero bezpečnostných zraniteľností

## Popis

Spoločnosť Aruba vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov spôsobiť zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

28.02.2023

## CVE

CVE-2022-4203, CVE-2022-4304, CVE-2022-4450, CVE-2023-0215, CVE-2023-0216, CVE-2023-0217, CVE-2023-0286, CVE-2023-0401

## Zasiahnuté systémy

AirWave Management Platform vo verzii staršej ako 8.3.0.1
Aruba Analytics and Location Engine vo verzii staršej ako 2.2.0.4
Aruba Central On-Premises (COP) vo verzii staršej ako 2.5.7.0
Aruba ClearPass Policy Manager - aktualizácia zatiaľ nie je dostupná
Aruba Fabric Composer (AFC) and Plexxi Composable Fabric Manager (CFM) vo verzii staršej ako 6.4.2
ArubaOS-CX Switches vo verzii staršej ako 10.11.1010, 10.10.1050, a 10.06.0240
ArubaOS SD-WAN Gateways
ArubaOS 8.6.x.x vo verzii staršej ako 8.6.0.21
ArubaOS 8.10.x.x vo verzii staršej ako 8.10.0.7
ArubaOS 8.11.x.x vo verzii staršej ako 8.11.1.0
ArubaOS 10.4.0.x vo verzii staršej ako 10.4.0.1
Aruba InstantOS / Aruba Access Points s operačným systémom ArubaOS 10
Aruba InstantOS 8.6.x.x vo verzii staršej ako 8.6.0.21
Aruba InstantOS 8.10.x.x vo verzii staršej ako 8.10.0.7
Aruba InstantOS 8.11.x.x vo verzii staršej ako 8.11.1.0
ArubaOS 10.4.0.x vo verzii staršej ako 10.4.0.1
Aruba EdgeConnect Enterprise - aktualizácia zatiaľ nie je dostupná
Aruba EdgeConnect Enterprise Orchestrator (on prem) - aktualizácia zatiaľ nie je dostupná

## Následky

Zneprístupnenie služby

| Odporúčania |
| --- |
| Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.<br>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.<br>Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu. Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN). |

| Zdroje |
| --- |
| https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-001.txt<br>https://nvd.nist.gov/vuln/detail/CVE-2022-4450 |

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

## Identifikátor

SolarWinds - viacero bezpečnostných zraniteľností

## Popis

Spoločnosť SolarWinds vydala bezpečnostnú aktualizáciu na svoju platformu SolarWinds Platform, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

17.02.2023

## CVE

CVE-2022-38111, CVE-2022-47503, CVE-2022-47504, CVE-2022-47506, CVE-2022-47507, CVE-2023-23836

## Zasiahnuté systémy

SolarWinds Platform vo verzii staršej ako 2023.1

## 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.solarwinds.com/trust-center/security-advisories/cve-2023-23836
https://www.securityweek.com/solarwinds-announces-upcoming-patches-for-high-severity-vulnerabilities/