# BEZPEČNOSTNÝ BULLETIN

Týždeň 08. 11. 2023 - 14. 11. 2023

## OBSAH BEZPEČNOSTNÉHO BULLETINU

| Č. | Identifikátor | Dôležitosť | CVSS Skóre |
|---|---|---|---|
| **01.** | ChromeOS - viacero bezpečnostných zraniteľností | Vysoká | **8.8** |
| **02.** | Chrome - bezpečnostná zraniteľnosť | Vysoká | **8.8** |
| **03.** | Apache UIMA - bezpečnostná zraniteľnosť | Vysoká | **8.8** |
| **04.** | Qnap produkty - viacero bezpečnostných zraniteľností | Vysoká | **8.8** |
| **05.** | Lanaccess ONSAFE MonitorHM - bezpečnostná zraniteľnosť | Vysoká | **8.8** |
| **06.** | NETGEAR NMS300 - bezpečnostná zraniteľnosť | Vysoká | **8.8** |
| **07.** | Mediatek produkty - viacero bezpečnostných zraniteľností | Vysoká | **8.4** |
| **08.** | EnBw SENEC legacy storage box - dve bezpečnostné zraniteľnosti | Vysoká | **8.1** |
| **09.** | Ivanti Secure Access Client - viacero bezpečnostných zraniteľností | Vysoká | **7.8** |
| **10.** | Fuji Electric produkty - viacero bezpečnostných zraniteľností | Vysoká | **7.8** |
| **11.** | VLC Media Player - dve bezpečnostné zraniteľnosti | Vysoká | **7.5** |
| **12.** | MS Edge - tri bezpečnostné zraniteľnosti | Vysoká | **7.3** |
| **13.** | MiCOM S1 Agile - bezpečnostná zraniteľnosť | Stredná | **5.3** |
| **14.** | Hitachi Energy eSOMS - tri bezpečnostné zraniteľnosti | Stredná | **5.3** |

**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-1408

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

## Identifikátor

ChromeOS - viacero bezpečnostných zraniteľností

## Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj produkt ChromeOS, 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

24.10.2023

## CVE

CVE-2023-21263, CVE-2023-21401, CVE-2023-35688, CVE-2023-38545, CVE-2023-5472, CVE-2023-5474, CVE-2023-5481

## Zasiahnuté systémy

Chrome OS LTS channel vo veryii staršej ako 114.0.5735.339 (Platform Version: 15437.76.0)

## 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://chromereleases.googleblog.com/2023/11/long-term-support-channel-update-for.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/269433

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

## Identifikátor

Chrome - bezpečnostná zraniteľnosť

## Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj prehliadač Chrome, ktorá opravuje bezpečnostnú zraniteľnosť.
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

07.11.2023

## CVE

CVE-2023-5996

## Zasiahnuté systémy

Chrome pre Mac a Linux vo verzii staršej ako 119.0.6045.123
Chrome pre Windows vo verzii staršej ako 119.0.6045.123/.124

## 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/2023/11/stable-channel-update-for-desktop.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/270767

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

## Identifikátor

Apache UIMA - bezpečnostná zraniteľnosť

## Popis

Vývojári štandardu Apache UIMA vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

08.11.2023

## CVE

CVE-2023-39913

## Zasiahnuté systémy

Apache UIMA Java SDK vo verzii staršej ako 3.5.0

## Následky

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

## Odporúčania

Administrátorom a používateľom odporúčame bezodkladne 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://lists.apache.org/thread/lw30f4qlq3mhkhplj16qw4fot3rg7v4
https://exchange.xforce.ibmcloud.com/vulnerabilities/270940

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

## Identifikátor

Qnap produkty - viacero bezpečnostných zraniteľností

## Popis

Spoločnosť Qnap vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v produkte QuMagie, 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

11.11.2023

## CVE

CVE-2023-23367, CVE-2023-39295, CVE-2023-41284, CVE-2023-41285

## Zasiahnuté systémy

QuMagie vo verzii staršej ako 2.1.3
QTS vo verzii staršej ako 5.0.1.2376 build 20230421
QuTS hero vo verzii staršej ako h5.0.1.2376 build 20230421
QuTScloud vo verzii staršej ako c5.1.0.2498

## 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.qnap.com/en/security-advisory/qsa-23-24
https://www.qnap.com/en/security-advisory/qsa-23-50
https://nvd.nist.gov/vuln/detail/CVE-2023-39295

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

## Identifikátor

Lanaccess ONSAFE MonitorHM - bezpečnostná zraniteľnosť

## Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu Lanaccess ONSAFE MonitorHM. Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

08.11.2023

## CVE

CVE-2023-6012

## Zasiahnuté systémy

Lanaccess ONSAFE MonitorHM vo verzii staršej ako 3.7.0 (vrátane)

## Následky

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

## Odporúčania

Vzhľadom na to, že produkt už nie je udržiavaný, odporúčame prejsť na iný produkt s platnou podporou.

## Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/271020

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

## Identifikátor

NETGEAR NMS300 - bezpečnostná zraniteľnosť

## Popis

Spoločnosť NETGEAR vydala bezpečnostnú aktualizáciu na svoj systém pre manažment sietí NMS300, ktorá opravuje bezpečnostnú zraniteľnosť.

Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby. Zraniteľnosť nemá pridelený identifikátor CVE.

## Dátum prvého zverejnenia varovania

13.11.2023

## CVE

-

## Zasiahnuté systémy

NMS300 vo verzii staršej ako 1.7.0.31

## 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://kb.netgear.com/000065866/Security-Advisory-for-Multiple-Vulnerabilities-on-the-NMS300-PSV-2023-0114-PSV-2023-0115?article=000065866
https://exchange.xforce.ibmcloud.com/vulnerabilities/271122

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

## Identifikátor

Mediatek produkty - viacero bezpečnostných zraniteľností

## Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach čipsetov Mediatek.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej aplikácie eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

05.11.2023

## CVE

CVE-2023-20702, CVE-2023-32818, CVE-2023-32825, CVE-2023-32832, CVE-2023-32834, CVE-2023-32835, CVE-2023-32836, CVE-2023-32837, CVE-2023-32838, CVE-2023-32839, CVE-2023-32840

## Zasiahnuté systémy

Mediatek čipsety prevádzkované s operačným systémom Android vo verzii 11.0, 12.0 a 13.0
Mediatek čipsety prevádzkované v modemoch NR15, NR16, NR17, VMOLYN, LR12A

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkaze v časti ZDROJE

## Následky

Eskalácia privilégií
Úplné narušenie dôvernosti, integrity a dostupnosti systému

## Odporúčania

Odporúčame uistiť sa, či Vaše zariadenia využívajúce čipsety MediaTek neprevádzkujú operačný systém Android v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu operačného systému.
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://corp.mediatek.com/product-security-bulletin/November-2023
https://exchange.xforce.ibmcloud.com/vulnerabilities/270586

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

## Identifikátor

EnBw SENEC legacy storage box - dve bezpečnostné zraniteľnosti

## Popis

Spoločnosť EnBw SENEC vydala bezpečnostnú aktualizáciu na svoj produkt legacy storage box, ktorá opravuje dve bezpečnostné zraniteľnosti.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom odpočúvania sieťovej prevádzky získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Na uvedenú zraniteľnosť je v súčasnosti voľne dostupný Proof-of-Concept kód.

## Dátum prvého zverejnenia varovania

13.11.2023

## CVE

CVE-2023-39167, CVE-2023-39168

## Zasiahnuté systémy

EnBw SENEC legacy storage box vo verzii firmvéru staršej ako 11. September 2023

## Následky

Neoprávnený prístup k citlivým údajom

Neoprávnená zmena v systéme

## 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://seclists.org/fulldisclosure/2023/Nov/4

https://exchange.xforce.ibmcloud.com/vulnerabilities/271248

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

## Identifikátor

Ivanti Secure Access Client - viacero bezpečnostných zraniteľností

## Popis

Spoločnosť Ivanti vydala bezpečnostnú aktualizáciu na svoj produkt Secure Access Client, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia 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 zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

09.11.2023

## CVE

CVE-2023-35080, CVE-2023-38043, CVE-2023-38543, CVE-2023-38544, CVE-2023-41718

## Zasiahnuté systémy

Secure Access Client vo verzii staršej ako 22.6R1

## 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://forums.ivanti.com/s/article/Security-fixes-included-in-the-latest-Ivanti-Secure-Access-Client-Release?language=en_US
https://exchange.xforce.ibmcloud.com/vulnerabilities/271125

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

## Identifikátor

Fuji Electric produkty - viacero bezpečnostných zraniteľností

## Popis

Spoločnosť Fuji Electric vydala bezpečnostné aktualizácie na svoje portfólio produktov Tellus a V-Server, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia 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. Zneužitie zraniteľnosti vyžaduje interakciu používateľa.

## Dátum prvého zverejnenia varovania

10.11.2023

## CVE

CVE-2023-47580, CVE-2023-47581, CVE-2023-47582, CVE-2023-47583, CVE-2023-47584, CVE-2023-47585, CVE-2023-47586

## Zasiahnuté systémy

Tellus produkty vo verzii staršej ako Ver.4.0.19.0
V-Server produkty vo verzii staršej ako Ver.4.0.19.0

## 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 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

http://jvn.jp/en/vu/JVNVU93840158/index.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/271133

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

## Identifikátor

VLC Media Player - dve bezpečnostné zraniteľnosti

## Popis

Spoločnosť Videolan vydala bezpečnostnú aktualizáciu na svoj produkt VLC Media Player, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia 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

07.11.2023

## CVE

CVE-2023-47359, CVE-2023-47360

## Zasiahnuté systémy

VLC vo verzii staršej ako 3.0.20

## Následky

Zneprístupnenie služby

## Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

## Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/271024
https://exchange.xforce.ibmcloud.com/vulnerabilities/271023

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

## Identifikátor

MS Edge - tri bezpečnostné zraniteľnosti

## Popis

Spoločnosť Microsoft vydala bezpečnostnú aktualizáciu na svoj internetový prehliadač Edge, ktorá opravuje tri bezpečnostné zraniteľnosti.
Najzávažnejšia 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

09.11.2023

## CVE

CVE-2023-36014, CVE-2023-36024, CVE-2023-36027

## Zasiahnuté systémy

Microsoft Edge Stable Channel vo verzii staršej ako 119.0.2151.58
Microsoft Edge Extended Stable Channel vo verzii staršej ako 118.0.2088.102

## 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://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36027
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36024
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36014
https://exchange.xforce.ibmcloud.com/vulnerabilities/271079
https://exchange.xforce.ibmcloud.com/vulnerabilities/271078

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☒ **Stredná** | ☐ **Vysoká** | ☐ **Kritická** | **CVSS skóre:** 5.3 |
| **Klasifikácia** | ☒ **Neutajované / TLP(CLEAR)** | | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

MiCOM S1 Agile - bezpečnostná zraniteľnosť

## Popis

Spoločnosť General Electric vydala automatickú bezpečnostnú aktualizáciu na svoj produkt MiCOM S1 Agile, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom zaslania špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

07.11.2023

## CVE

CVE-2023-0898

## Zasiahnuté systémy

General Electric MiCOM S1 Agile vo všetkých verziách

## Následky

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

## Odporúčania

Pre vykonanie aktualizácie nie je zo strany používateľa potrebná žiadna akcia.
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-23-311-23

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☒ **Stredná** | ☐ **Vysoká** | ☐ **Kritická** | **CVSS skóre:** 5.3 |
| **Klasifikácia** | ☒ **Neutajované / TLP(CLEAR)** | | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

Hitachi Energy eSOMS - tri bezpečnostné zraniteľnosti

## Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktu eSOMS.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom.

## Dátum prvého zverejnenia varovania

09.11.2023

## CVE

CVE-2023-5514, CVE-2023-5515, CVE-2023-5516

## Zasiahnuté systémy

eSOMS vo verzii staršej ako v6.3.13 (vrátane)

## Následky

Neoprávnený prístup k citlivým údajom

## Odporúčania

Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat 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://publisher.hitachienergy.com/preview?DocumentId=8DBD000175&languageCode=en&Preview=true
https://www.cisa.gov/news-events/ics-advisories/icsa-23-313-02