# BEZPEČNOSTNÝ BULLETIN

Týždeň 23. 08. 2023 - 29. 08. 2023

## OBSAH BEZPEČNOSTNÉHO BULLETINU

| Č. | Identifikátor | Dôležitosť | CVSS Skóre |
|---|---|---|---|
| **01.** | TP-Link smart žiarovky - viacero bezpečnostných zraniteľností | Vysoká | **8.8** |
| **02.** | NETGEAR RAX30 - tri bezpečnostné zraniteľnosti | Vysoká | **8.8** |
| **03.** | TP-Link produkty - viacero bezpečnostných zraniteľností | Vysoká | **8.8** |
| **04.** | Kubernetes - tri bezpečnostné zraniteľnosti | Vysoká | **8.8** |
| **05.** | Google Chrome - viacero bezpečnostných zraniteľností | Vysoká | **8.8** |
| **06.** | HP Tlačiarne - bezpečnostná zraniteľnosť | Vysoká | **8.8** |
| **07.** | ASUSTOR Data Master - bezpečnostná zraniteľnosť | Vysoká | **8.7** |
| **08.** | Rockwell Automation I/O moduly - bezpečnostná zraniteľnosť | Vysoká | **8.6** |
| **09.** | HPE Aruba EdgeConnect SD-WAN Orchestrator - viacero bezpečnostných zraniteľností | Vysoká | **8.1** |
| **10.** | McAfee Safe Connect VPN - bezpečnostná zraniteľnosť | Vysoká | **7.8** |
| **11.** | openSUSE-welcome - bezpečnostná zraniteľnosť | Vysoká | **7.8** |
| **12.** | 7-Zip - bezpečnostná zraniteľnosť | Vysoká | **7.8** |
| **13.** | WinRAR - bezpečnostná zraniteľnosť | Vysoká | **7.8** |
| **14.** | Cisco produkty - viacero bezpečnostných zraniteľností | Vysoká | **7.8** |
| **15.** | Avira Free Antivirus - bezpečnostná zraniteľnosť | Vysoká | **7.8** |
| **16.** | Apache Airflow - bezpečnostná zraniteľnosť | Vysoká | **7.6** |
| **17.** | KNX zariadenia - bezpečnostná zraniteľnosť | Vysoká | **7.5** |
| **18.** | OPTO 22 SNAP PAC S1 - viacero bezpečnostných zraniteľností | Vysoká | **7.5** |
| **19.** | Qnap produkty - tri bezpečnostné zraniteľnosti | Vysoká | **7.1** |
| **20.** | 3CX - bezpečnostná zraniteľnosť | Vysoká | **7.0** |
| **21.** | Trane termostaty - bezpečnostná zraniteľnosť | Stredná | **6.8** |

**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-1300

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

## Identifikátor

TP-Link smart žiarovky - viacero bezpečnostných zraniteľností

## Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach smart žiaroviek Tapo L530E od firmy TP-Link.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

17.08.2023

## CVE

CVE-2023-38906, CVE-2023-38908, CVE-2023-38909

## Zasiahnuté systémy

Tapo L530B a Tapo L530E s firmvérom vo verzii 1.0.X a starších verziách
Tapo mobilná aoplikácia vo verzii 2.17.X a starších verziách

## Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému

## Odporúčania

Výrobca postupne vydáva bezpečnostné aktualizácie na predmetné zraniteľnosti. 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://www.tp-link.com/en/support/faq/3722/
https://arxiv.org/pdf/2308.09019.pdf
https://www.bleepingcomputer.com/news/security/tp-link-smart-bulbs-can-let-hackers-steal-your-wifi-password/

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

## Identifikátor

NETGEAR RAX30 - tri bezpečnostné zraniteľnosti

## Popis

Spoločnosť NETGEAR vydala bezpečnostnú aktualizáciu na svoj router RAX30, ktorá opravuje tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje útočníkovi nachádzajúcemu sa 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

22.08.2023

## CVE

CVE-2023-40478, CVE-2023-40479, CVE-2023-40480

## Zasiahnuté systémy

RAX30 vo verzii firmvéru staršej ako 1.0.9.92

## 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.zerodayinitiative.com/advisories/ZDI-23-1161/
https://www.zerodayinitiative.com/advisories/ZDI-23-1162/
https://www.zerodayinitiative.com/advisories/ZDI-23-1163/

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

## Identifikátor

TP-Link produkty - viacero bezpečnostných zraniteľností

## Popis

Spoločnosť TP-Link vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi, 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

21.08.2023

## CVE

CVE-2022-24355, CVE-2023-31188, CVE-2023-32619, CVE-2023-36489, CVE-2023-37284, CVE-2023-38563, CVE-2023-38568, CVE-2023-38588, CVE-2023-39224, CVE-2023-39935, CVE-2023-40193, CVE-2023-40357, CVE-2023-40531

## Zasiahnuté systémy

Archer C50 vo verzii firmvéru staršej ako Archer C50(JP)_V3_230505
Archer C55 vo verzii firmvéru staršej ako Archer C55(JP)_V1_230506
TL-WR802N vo verzii firmvéru staršej ako TL-WR802N(JP)_V4_221008
TL-WR841N vo verzii firmvéru staršej ako TL-WR841N(JP)_V14_230506
TL-WR902AC vo verzii firmvéru staršej ako TL-WR902AC(JP)_V3_230506
Archer C20 vo verzii firmvéru staršej ako Archer C20(JP)_V1_230616
Archer C1200 vo verzii firmvéru staršej ako Archer C1200(JP)_V2_230508
Archer C9 vo verzii firmvéru staršej ako Archer C9(JP)_V3_230508
Archer A10 vo verzii firmvéru staršej ako Archer A10(JP)_V2_230504
Archer C3150 vo verzii firmvéru staršej ako Archer C3150(JP)_V2_230511
Archer C5 vo všetkých verziách firmvéru
Archer C7 vo verzii firmvéru staršej ako Archer C7(JP)_V2_230602
Archer C5400 vo verzii firmvéru staršej ako Archer C5400(JP)_V2_230506
TL-WR940N vo verzii firmvéru staršej ako TL-WR940N(JP)_V6_201103
Deco M4 vo verzii firmvéru staršej ako Deco M4(JP)_V2_1.5.8 Build 20230619
Archer AX50 vo verzii firmvéru staršej ako Archer AX50(JP)_V1_230529
Archer AX10 vo verzii firmvéru staršej ako Archer AX10(JP)_V1.2_230508
Archer AX11000 vo verzii firmvéru staršej ako Archer AX11000(JP)_V1_230523
Archer AX6000 vo verzii firmvéru staršej ako Archer AX6000(JP)_V1_1.3.0 Build 20221208

## Následky

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

| Odporúčania |
| --- |
| Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.<br>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 |
| --- |
| http://jvn.jp/en/vu/JVNVU99392903/index.html |

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

## Identifikátor

Kubernetes - tri bezpečnostné zraniteľnosti

## Popis

Vývojári platformy Kubernetes vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje tri bezpečnostné zraniteľnosti.
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

23.08.2023

## CVE

CVE-2023-3676, CVE-2023-3893, CVE-2023-3955

## Zasiahnuté systémy

kubelet vo verzii staršej ako master
kubelet vo verzii staršej ako v1.28.1
kubelet vo verzii staršej ako v1.27.5
kubelet vo verzii staršej ako v1.26.8
kubelet vo verzii staršej ako v1.25.13
kubelet vo verzii staršej ako v1.24.17

## 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://exchange.xforce.ibmcloud.com/vulnerabilities/264233
https://exchange.xforce.ibmcloud.com/vulnerabilities/264230
https://exchange.xforce.ibmcloud.com/vulnerabilities/264229

| | | | | | |
|---|---|---|---|---|---|
| **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

22.08.2023

## CVE

CVE-2023-4427, CVE-2023-4428, CVE-2023-4429, CVE-2023-4430, CVE-2023-4431

## Zasiahnuté systémy

Chrome pre Mac a Linux vo verzii staršej ako 116.0.5845.110
Chrome pre Windows vo verzii staršej ako 116.0.5845.110/.111

## 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/2023/08/chrome-desktop-stable-update.html

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

## Identifikátor

HP Tlačiarne - bezpečnostná zraniteľnosť

## Popis

Spoločnosť Hewlett Packard vydala bezpečnostnú aktualizáciu na svoje portfólio tlačiarní, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente prostredníctvom pretečenia zásobníka vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

24.08.2023

## CVE

CVE-2023-27971

## Zasiahnuté systémy

HP ENVY 6000e All-In-One Printer series vo verzii firmvéru staršej ako 001.2323A
HP ENVY 6400e All-In-One Printer series vo verzii firmvéru staršej ako 001.2323A
HP ENVY Inspire 7200e series vo verzii firmvéru staršej ako 002.2313B
HP ENVY Inspire 7900 series vo verzii firmvéru staršej ako 002.2313B
HP ENVY Inspire 7900e series vo verzii firmvéru staršej ako 002.2313B
HP Color LaserJet MFP M478-M479 series vo verzii firmvéru staršej ako 002_2310A
HP Color LaserJet Pro M453-M454 series vo verzii firmvéru staršej ako 002_2310A
HP LaserJet Pro 3001-3008dn/dw Printer Series vo verzii firmvéru staršej ako 2314A
HP LaserJet Pro 4001-4004n/dn/dw/d Printer Series vo verzii firmvéru staršej ako 2314A
HP LaserJet Pro M304-M305 Printer series vo verzii firmvéru staršej ako 002_2310A
HP LaserJet Pro M404-M405 Printer series vo verzii firmvéru staršej ako 002_2310A
HP LaserJet Pro MFP 3100-3108fdn/fdw Series vo verzii firmvéru staršej ako 2314A
HP LaserJet Pro MFP 4101-4104dw/fdn/fdw Printer Series vo verzii firmvéru staršej ako 2314A
HP LaserJet Pro MFP M428-M429 f series vo verzii firmvéru staršej ako 002_2310A
HP LaserJet Pro MFP M428-M429 series vo verzii firmvéru staršej ako 002_2310A
HP OfficeJet Pro 7740 Wide Format All-in-One Printer series vo verzii firmvéru staršej ako 002.2312A
HP PageWide 352dw Printer vo verzii firmvéru staršej ako 2313A
HP PageWide 377dw Multifunction Printer vo verzii firmvéru staršej ako 2313A
HP PageWide Managed P55250dw Printer series vo verzii firmvéru staršej ako 2313A
HP PageWide Managed P57750dw Multifunction Printer vo verzii firmvéru staršej ako 2313A
HP PageWide Pro 452dn Printer series vo verzii firmvéru staršej ako 2313A
HP PageWide Pro 452dw Printer series vo verzii firmvéru staršej ako 2313A
HP PageWide Pro 477dn Multifunction Printer series vo verzii firmvéru staršej ako 2313A
HP PageWide Pro 477dw Multifunction Printer series vo verzii firmvéru staršej ako 2313A
HP PageWide Pro 552dw Printer series vo verzii firmvéru staršej ako 2313A
HP PageWide Pro 577 Multifunction Printer series vo verzii firmvéru staršej ako 2313A

| Následky |
| --- |
| Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému |

| Odporúčania |
| --- |
| Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.<br>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.hp.com/us-en/document/ish_7919962-7920003-16/hpsbpi03839<br>https://www.zerodayinitiative.com/advisories/ZDI-23-1178/ |

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☐ **Stredná** | ☒ **Vysoká** | ☐ **Kritická** | **CVSS skóre:** 8.7 |
| **Klasifikácia** | ☒ **Neutajované / TLP(CLEAR)** | | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

ASUSTOR Data Master - bezpečnostná zraniteľnosť

## Popis

Spoločnosť ASUSTOR vydala bezpečnostnú aktualizáciu na svoj produkt Data Master, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, 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

23.08.2023

## CVE

CVE-2023-3699

## Zasiahnuté systémy

ADM vo verzii staršej ako 4.2.3.RK91

## 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://www.asustor.com/security/security_advisory_detail?id=29
https://exchange.xforce.ibmcloud.com/vulnerabilities/264150

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

## Identifikátor

Rockwell Automation I/O moduly - bezpečnostná zraniteľnosť

## Popis

Spoločnosť Rockwell Automation vydala bezpečnostné aktualizácie na svoje portfólio I/O modulov, 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

24.08.2023

## CVE

CVE-2022-1737

## Zasiahnuté systémy

- 1734-AENT/1734-AENTR Series C vo verzii staršej ako 7.013
- 1734-AENT/1734-AENTR Series B vo verzii staršej ako 5.021
- 1738-AENT/ 1738-AENTR Series B vo verzii staršej ako 6.013
- 1794-AENTR Series A vo verzii staršej ako 2.012
- 1732E-16CFGM12QCWR Series A vo verzii staršej ako 3.012
- 1732E-12X4M12QCDR Series A vo verzii staršej ako 3.012
- 1732E-16CFGM12QCR Series A vo verzii staršej ako 3.012
- 1732E-16CFGM12P5QCR Series A vo verzii staršej ako 3.012
- 1732E-12X4M12P5QCDR Series A vo verzii staršej ako 3.012
- 1732E-16CFGM12P5QCWR Series B vo verzii staršej ako 3.012
- 1732E-IB16M12R Series B vo verzii staršej ako 3.012
- 1732E-OB16M12R Series B vo verzii staršej ako 3.012
- 1732E-16CFGM12R Series B vo verzii staršej ako 3.012
- 1732E-IB16M12DR Series B vo verzii staršej ako 3.012
- 1732E-OB16M12DR Series B vo verzii staršej ako 3.012
- 1732E-8X8M12DR Series B vo verzii staršej ako 3.012
- 1799ER-IQ10XOQ10 Series B vo verzii staršej ako 3.012

## 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-23-236-06 |

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

## Identifikátor

HPE Aruba EdgeConnect SD-WAN Orchestrator - viacero bezpečnostných zraniteľností

## Popis

Spoločnosť Hewlett Packard Enterprise vydala bezpečnostné aktualizácie na svoje portfólio produktov EdgeConnect SD-WAN Orchestrator, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť 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

24.08.2023

## CVE

CVE-2023-37421, CVE-2023-37422, CVE-2023-37423, CVE-2023-37424, CVE-2023-37425, CVE-2023-37426, CVE-2023-37427, CVE-2023-37428, CVE-2023-37429, CVE-2023-37430, CVE-2023-37431, CVE-2023-37432, CVE-2023-37433, CVE-2023-37434, CVE-2023-37435, CVE-2023-37436, CVE-2023-37437, CVE-2023-37438, CVE-2023-37439, CVE-2023-37440

## Zasiahnuté systémy

EdgeConnect SD-WAN Orchestrator 9.3.x vo verzii staršej ako 9.3.1
EdgeConnect SD-WAN Orchestrator 9.2.x vo verzii staršej ako 9.2.6
EdgeConnect SD-WAN Orchestrator 9.1.x vo verzii staršej ako 9.1.8
EdgeConnect SD-WAN Orchestrator vo verzii staršej ako 9.0.x (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://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04531en_us

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

## Identifikátor

McAfee Safe Connect VPN - bezpečnostná zraniteľnosť

## Popis

Spoločnosť McAfee vydala bezpečnostnú aktualizáciu na svoj produkt Safe Connect VPN, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom podvrhnutia špeciálne vytvorených DLL súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

18.08.2023

## CVE

CVE-2023-40352

## Zasiahnuté systémy

McAfee Safe Connect vo verzii staršej ako 2.16.1.126

## 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.mcafee.com/support/?articleId=TS103462&page=shell&shell=article-view
https://www.zerodayinitiative.com/advisories/ZDI-23-1158/

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

## Identifikátor

openSUSE-welcome - bezpečnostná zraniteľnosť

## Popis

Vývojári nástroja openSUSE-welcome 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 vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

22.08.2023

## CVE

CVE-2023-32184

## Zasiahnuté systémy

openSUSE-welcome vo verzii staršej ako 0.1.9+git.35.4b9444a

## 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://seclists.org/oss-sec/2023/q3/117
https://exchange.xforce.ibmcloud.com/vulnerabilities/264132

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

## Identifikátor

7-Zip - bezpečnostná zraniteľnosť

## Popis

Vývojári nástroja 7-Zip vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje dve 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.
Zneužitie zraniteľnosti vyžaduje interakciu používateľa.

## Dátum prvého zverejnenia varovania

23.08.2023

## CVE

CVE-2023-31102, CVE-2023-40481

## Zasiahnuté systémy

7-Zip vo verzii staršej ako 23.00

## 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.zerodayinitiative.com/advisories/ZDI-23-1164/
https://www.zerodayinitiative.com/advisories/ZDI-23-1165/

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

## Identifikátor

WinRAR - bezpečnostná zraniteľnosť

## Popis

Spoločnosť win.rar vydala bezpečnostnú aktualizáciu na svoj produkt WinRAR, ktorá opravuje bezpečnostnú zraniteľnosť.
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

23.08.2023

## CVE

CVE-2023-38831

## Zasiahnuté systémy

WinRAR vo verzii staršej ako 6.23

## 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.win-rar.com/singlenewsview.html?&L=0&tx_ttnews%5Btt_news%5D=232&cHash=c5bf79590657e32554c6683296a8e8aa
https://exchange.xforce.ibmcloud.com/vulnerabilities/264175

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

## Identifikátor

Cisco produkty - viacero bezpečnostných zraniteľností

## Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne upravených príkazov eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

23.08.2023

## CVE

CVE-2023-20168, CVE-2023-20169, CVE-2023-20197, CVE-2023-20200, CVE-2023-20217, CVE-2023-20224

## Zasiahnuté systémy

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkazoch v sekcii ZDROJE

## Následky

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

## 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.
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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-remoteauth-dos-XB6pv74m<br>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-thoueye-privesc-NVhHGwb3<br>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fp-ucsfi-snmp-dos-qtv69NAO<br>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-n3_9k-isis-dos-FTCXB4Vb<br>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-rNwNEEee<br>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-remoteauth-dos-XB6pv74m |

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

## Identifikátor

Avira Free Antivirus - bezpečnostná zraniteľnosť

## Popis

Spoločnosť Symantec vydala bezpečnostnú aktualizáciu na svoj produkt Avira Free Antivirus, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

24.08.2023

## CVE

CVE-2023-1900

## Zasiahnuté systémy

Avira Antivirus pre Windows Endpointprotection.exe vo verzii staršej ako 1.0.2303.633

## Následky

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

## 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.zerodayinitiative.com/advisories/ZDI-23-1169/
https://support.norton.com/sp/static/external/tools/security-advisories.html

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☐ **Stredná** | ☒ **Vysoká** | ☐ **Kritická** | **CVSS skóre:** 7.6 |
| **Klasifikácia** | ☒ **Neutajované / TLP(CLEAR)** | | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

Apache Airflow - bezpečnostná zraniteľnosť

## Popis

Vývojári platformy Apache Airflow 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 získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

23.08.2023

## CVE

CVE-2023-37379

## Zasiahnuté systémy

Apache Airflow vo verzii staršej ako 2.7.0

## Následky

Neoprávnený prístup k citlivým údajom
Zneprístupnenie služby
Vykonanie škodlivého kódu

## 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/264232

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

## Identifikátor

KNX zariadenia - bezpečnostná zraniteľnosť

## Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti zariadení KNX.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky spôsobiť zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

24.08.2023

## CVE

CVE-2023-4346

## Zasiahnuté systémy

KNX zariadenia využívajúce Connection Authorization Option 1 Style v ktorom nie je nastavený BCU kľúč vo všetkých verziách

## Následky

Zneprístupnenie služby

## Odporúčania

Administrátorom odporúčame postupovať podľa pokynov výrobcu, ktoré môžete nájsť na webovej adrese:
https://www.knx.org/knx-en/for-professionals/benefits/knx-secure/index.php
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-23-236-01

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

## Identifikátor

OPTO 22 SNAP PAC S1 - viacero bezpečnostných zraniteľností

## Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktu SNAP PAC S1.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať brute-force útok a získať neoprávnený prístup k citlivým údajom.

## Dátum prvého zverejnenia varovania

24.08.2023

## CVE

CVE-2023-40706, CVE-2023-40707, CVE-2023-40708, CVE-2023-40709, CVE-2023-40710

## Zasiahnuté systémy

SNAP PAC S1 s firmvérom vo verzii staršej ako R10.3b (vrátane)

## Následky

Neoprávnený prístup k citlivým údajom
Zneprístupnenie služby

## Odporúčania

Na uvedené zraniteľnosti v súčasnosti nie sú dostupné bezpečnostné aktualizácie. Administrátorom odporúčame postupovať podľa pokynov výrobcu, ktoré môžete nájsť na webovej adrese: https://www.cisa.gov/news-events/ics-advisories/icsa-23-236-02 v časti 4.MITIGATIONS.

## Zdroje

https://www.cisa.gov/news-events/ics-advisories/icsa-23-236-02

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☐ **Stredná** | ☒ **Vysoká** | ☐ **Kritická** | **CVSS skóre:** 7.1 |
| **Klasifikácia** | ☒ **Neutajované / TLP(CLEAR)** | | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

Qnap produkty - tri bezpečnostné zraniteľnosti

## Popis

Spoločnosť Qnap vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente vykonať brute-force útok a získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

24.08.2023

## CVE

CVE-2023-34971, CVE-2023-34972, CVE-2023-34973

## Zasiahnuté systémy

QTS 5.0.1.2425 vo verzii staršej ako 20230609
QTS 5.1.0.2444 vo verzii staršej ako 20230629
QTS 4.5.4.2467 vo verzii staršej ako 20230718
QuTS hero h5.1.0.2424 vo verzii staršej ako 20230609
QuTS hero h4.5.4.2476 vo verzii staršej ako 20230728

## Následky

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://github.com/advisories/GHSA-8f9x-x39g-28fc
https://www.qnap.com/en/security-advisory/qsa-23-60
https://www.qnap.com/en/security-advisory/qsa-23-59
https://www.qnap.com/en/security-advisory/qsa-23-58

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☐ **Stredná** | ☒ **Vysoká** | ☐ **Kritická** | **CVSS skóre: 7.0** |
| **Klasifikácia** | ☒ **Neutajované / TLP(CLEAR)** | | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

3CX - bezpečnostná zraniteľnosť

## Popis

Spoločnosť 3CX vydala bezpečnostnú aktualizáciu na svoj rovnomenný produkt, ktorá opravuje bezpečnostnú zraniteľnosť.
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

21.08.2023

## CVE

CVE-2023-27362

## Zasiahnuté systémy

3CX vo verzii staršej ako 18.0 Update 8 Final

## 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.zerodayinitiative.com/advisories/ZDI-23-1153/
https://www.3cx.com/blog/releases/v18-u8/

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☒ **Stredná** | ☐ **Vysoká** | ☐ **Kritická** | **CVSS skóre:** 6.8 |
| **Klasifikácia** | ☒ **Neutajované / TLP(CLEAR)** | | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

Trane termostaty - bezpečnostná zraniteľnosť

## Popis

Spoločnosť Trane vydala bezpečnostnú aktualizáciu firmvéru na svoje produkty XL824, XL850, XL1050 a Pivot, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi s fyzickým prístupom k zariadeniu prostredníctvom injekcie špeciálne upravených príkazov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

22.08.2023

## CVE

CVE-2023-4212

## Zasiahnuté systémy

Trane Technologies XL824 Thermostat vo verzii firmvéru staršej ako 5.9.8 (vrátane)
Trane Technologies XL850 Thermostat vo verzii firmvéru staršej ako 5.9.8 (vrátane)
Trane Technologies XL1050 Thermostat vo verzii firmvéru staršej ako 5.9.8 (vrátane)
Trane Technologies Pivot Thermostat vo verzii firmvéru staršej ako 1.8 (vrátane)

## Následky

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

## Odporúčania

Aktualizácia firmvéru predmetných produktov prebehne automaticky, pre jej spustenie stačí aktívne pripojenie k internetu.
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-23-234-02