# BEZPEČNOSTNÝ BULLETIN

Týždeň 27. 03. 2024 - 02. 04. 2024

## OBSAH BEZPEČNOSTNÉHO BULLETINU



**Národný bezpečnostný úrad**
Budatínska 30
851 06 Bratislava

Mail: *sk-cert@nbu.gov.sk*
Mobil: *+421 903 993 706*
Tel: *+421 2 6869 2915*

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

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

## Identifikátor

TRENDnet AC1200 - tri bezpečnostné zraniteľnosti

## Popis

Spoločnosť TRENDnet vydala bezpečnostnú aktualizáciu na svoj produkt TRENDnet AC1200 TEW-821DAP, ktorá opravuje tri bezpečnostné zraniteľnosti.
Bezpečnostné zraniteľnosti s identifikátormi CVE-2023-51146, CVE-2023-51147, CVE-2023-51148 spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky 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

25.3.2024

## CVE

CVE-2023-51146, CVE-2023-51147, CVE-2023-51148

## Zasiahnuté systémy

TRENDnet AC1200 TEW-821DAP s firmvérom vo verzii staršej ako 3.02B04

## Následky

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

## Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
SK-CERT administrátorom odporúča venovať osobitnú pozornosť aktualizácii firmvéru, nie len aplikačnému softvéru.

## Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/286455
https://exchange.xforce.ibmcloud.com/vulnerabilities/286456
https://exchange.xforce.ibmcloud.com/vulnerabilities/286457

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

## Identifikátor

Furuno Systems ACERA 9010 - bezpečnostná zraniteľnosť

## Popis

Spoločnosť Furuno Systems vydala bezpečnostnú aktualizácie na svoje prepínače ACERA 9010-08 a ACERA 9010-24, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-28744 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente získať úplnú kontrolu nad systémom. Zraniteľnosť je možné zneužiť na prepínačoch ACERA s počiatočnou konfiguráciou z výroby, ktoré aktívne nepracujú v režime MS.

## Dátum prvého zverejnenia varovania

1.4.2024

## CVE

CVE-2024-28744

## Zasiahnuté systémy

ACERA 9010-08 vo verzii firmvéru vo verzii staršej ako (vrátane) v02.04
ACERA 9010-24 vo verzii firmvéru vo verzii staršej ako (vrátane) v02.04

## Následky

Neoprávnený prístup do systému
Úplné narušenie dôvernosti, integrity a dostupnosti systému

## Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
V prípade, že aktualizácia systému nie je možná, odporúčame nastaviť ochranu heslom pomocou príkazov v CLI.
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.
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://jvn.jp/en/vu/JVNVU99285099/index.html
https://www.furunosystems.co.jp/news/info/vulner20240401.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/286686

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

## Identifikátor

Link Whisper Free WP plugin - bezpečnostná zraniteľnosť

## Popis

Vývojári Link Whisper Free pluginu pre WordPress vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-2693 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom injekcie PHP objektu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Ak je v zasiahnutom systéme prítomný POP chain, napríklad prostredníctvom iného nainštalovaného pluginu, možno predmetnú zraniteľnosť zneužiť na odstránenie ľubovoľných súborov v zasiahnutom systéme, neoprávnený prístup k citlivým údajom a vzdialené vykonanie kódu.

## Dátum prvého zverejnenia varovania

26.3.2024

## CVE

CVE-2024-2693

## Zasiahnuté systémy

Link Whisper Free vo verzii staršej ako 0.7.2

## Následky

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

## Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky a aplikácie založené na redakčnom systéme WordPress nevyužívajú predmetný plugin v zraniteľnej verzii. V prípade, že áno, bezodkladne zabezpečte aktualizáciu redakčného systému a všetkých používaných pluginov na aktuálne verzie bez známych bezpečnostných zraniteľností.
Po odstránení zraniteľností, ktoré mohli spôsobiť 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.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/link-whisper/link-whisper-free-071-authenticated-contributor-php-object-injection

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

## Identifikátor

Rockwell Automation produkty - viacero bezpečnostných zraniteľností

## Popis

Spoločnosť Rockwell Automation vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2024-21912 sa nachádza v produkte Arena Simulation Software, 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. Zneužitie zraniteľnosti vyžaduje interakciu používateľa.
Zneužitím ostatných bezpečnostných zraniteľností možno vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

26.3.2024

## CVE

CVE-2024-2425, CVE-2024-2426, CVE-2024-2427, CVE-2024-21914, CVE-2024-21912, CVE-2024-21913, CVE-2024-2929, CVE-2024-21918, CVE-2024-21919, CVE-2024-21920,

## Zasiahnuté systémy

Arena Simulation Software vo verzii staršej ako 16.20.03
PowerFlex 527 vo verzii staršej ako v2.001.x (vrátane)
FactoryTalk View ME vo verzii staršej ako v14

## Následky

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

## Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

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.
Detailné inštrukcie môžete nájsť na webovej adrese: https://www.rockwellautomation.com/en-us/support/advisory.SD1664.html

## Zdroje

https://www.cisa.gov/news-events/ics-advisories/icsa-24-086-03
https://www.cisa.gov/news-events/ics-advisories/icsa-24-086-04
https://www.cisa.gov/news-events/ics-advisories/icsa-24-086-02

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

## Identifikátor

phpMyFAQ - viacero bezpečnostných zraniteľností

## Popis

Vývojári open source webovej aplikácie phpMyFAQ vydali bezpečnostnú aktualizáciu na svoj produkt, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2024-27299 spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom SQL injekcie vykonať škodlivý kód a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.
Ostatné bezpečnostné zraniteľnosti možno zneužiť na neoprávnený prístup k citlivým údajom, neoprávnené zmeny v systéme, zneprístupnenie služby a vzdialené vykonanie škodlivého kódu. Zneužitie zraniteľností s identifikátormi CVE-2024-28108, CVE-2024-27300 a CVE-2024-28106 vyžaduje interakciu zo strany používateľa.

## Dátum prvého zverejnenia varovania

25.3.2024

## CVE

CVE-2024-27299, CVE-2024-28107, CVE-2024-28105, CVE-2024-28108, CVE-2024-27300, CVE-2024-28106

## Zasiahnuté systémy

phpMyFAQ vo verzii staršej ako 3.2.6

## Následky

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

## Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom alebo vzdialené vykonanie kódu, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

## Zdroje

https://www.phpmyfaq.de/security/advisory-2024-03-25
https://exchange.xforce.ibmcloud.com/vulnerabilities/286236
https://exchange.xforce.ibmcloud.com/vulnerabilities/286227
https://exchange.xforce.ibmcloud.com/vulnerabilities/286250
https://exchange.xforce.ibmcloud.com/vulnerabilities/286225
https://exchange.xforce.ibmcloud.com/vulnerabilities/286223
https://exchange.xforce.ibmcloud.com/vulnerabilities/286221

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

## Identifikátor

Autodesk produkty - dve bezpečnostné zraniteľnosti

## Popis

Spoločnosť Autodesk vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú dve bezpečnostné zraniteľnosti.
Bezpečnostné zraniteľnosti s identifikátormi CVE-2024-23139 a CVE-2024-23138 spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených ABC a DWG súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Zneužitie zraniteľností vyžaduje interakciu používateľa.

## Dátum prvého zverejnenia varovania

22.3.2024

## CVE

CVE-2024-23139, CVE-2024-23138

## Zasiahnuté systémy

Autodesk Advance Steel
Autodesk AutoCAD
Autodesk AutoCAD Architecture
Autodesk AutoCAD Electrical
Autodesk AutoCAD LT
Autodesk AutoCAD LT for Mac
Autodesk AutoCAD Mac
Autodesk AutoCAD Map 3D
Autodesk AutoCAD Mechanical
Autodesk AutoCAD MEP
Autodesk AutoCAD Plant 3D
Autodesk Civil 3D
Autodesk FBX Review
DWG TrueView
Free Autodesk Viewer

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkaze v časti ZDROJE

## Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Zneprístupnenie služby

## Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

## Zdroje

https://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0005
https://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0006

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

## Identifikátor

Linux Ubuntu - viacero bezpečnostných zraniteľností

## Popis

Vývojári Linux distribúcie Ubuntu vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje štyri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2023-27635 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených .deb súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Zneužitie zraniteľnosti vyžaduje interakciu zo strany používateľa.
Ostatné bezpečnostné zraniteľnosti možno zneužiť na zneprístupnenie služby, neoprávnený prístup k citlivým údajom, neoprávnené zmeny v systéme a vykonanie škodlivé kódu s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

26.3.2024

## CVE

CVE-2021-47154, CVE-2020-35459, CVE-2024-24246, CVE-2023-27635

## Zasiahnuté systémy

Ubuntu 23.10
debian-goodies - 0.88.1ubuntu1.2
libqpdf29 - 11.5.0-1ubuntu1.1
qpdf - 11.5.0-1ubuntu1.1

Ubuntu 22.04
debian-goodies - 0.87ubuntu1.1

Ubuntu 20.04
libnet-cidr-lite-perl vo verzii staršej ako 0.21-2ubuntu0.1
debian-goodies - 0.84ubuntu0.1
crmsh - 4.2.0-2ubuntu1.1

## Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
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 alebo vzdialené vykonanie kódu, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

## Zdroje

https://ubuntu.com/security/notices/USN-6712-1
https://ubuntu.com/security/notices/USN-6711-1
https://ubuntu.com/security/notices/USN-6713-1
https://ubuntu.com/security/notices/USN-6714-1

**Národný bezpečnostný úrad**
Budatínska 30
851 06 Bratislava

Mail: *sk-cert@nbu.gov.sk*
Mobil: *+421 903 993 706*
Tel: *+421 2 6869 2915*

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

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

## Identifikátor

Red Hat produkty - viacero bezpečnostných zraniteľností

## Popis

Spoločnosť Red Hat vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2024-29944 sa nachádza v produktoch Red Hat Enterprise Linux Client, Red Hat Enterprise Linux AppStream EUS a Red Hat Enterprise Linux AppStream AUS, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webovej stránky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Zneužitie zraniteľnosti vyžaduje interakciu používateľa.
Zneužitím ostatných bezpečnostných zraniteľností možno vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

25.3.2024

## CVE

CVE-2023-5388, CVE-2023-6185, CVE-2023-6186, CVE-2024-0743, CVE-2024-1394, CVE-2024-1936, CVE-2024-2607, CVE-2024-2608, CVE-2024-2610, CVE-2024-2611, CVE-2024-2612, CVE-2024-2614, CVE-2024-2616, CVE-2024-29944

## Zasiahnuté systémy

Red Hat Enterprise Linux AppStream
Red Hat Enterprise Linux AppStream AUS
Red Hat Enterprise Linux AppStream E4S
Red Hat Enterprise Linux AppStream EUS
Red Hat Enterprise Linux AppStream TUS
Red Hat Enterprise Linux Client (v. 7)
Red Hat Enterprise Linux Client Optional (v. 7)
Red Hat Enterprise Linux Server (v. 7)
Red Hat Enterprise Linux Server Optional (v. 7)
Red Hat Enterprise Linux Workstation (v. 7)
Red Hat Enterprise Linux Workstation Optional (v. 7)

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkaze v sekcii ZDROJE

## Následky

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

## Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

## Zdroje

https://access.redhat.com/errata/RHSA-2024:1490
https://access.redhat.com/errata/RHSA-2024:1487
https://access.redhat.com/errata/RHSA-2024:1489

**Národný bezpečnostný úrad**
Budatínska 30
851 06 Bratislava

Mail: *sk-cert@nbu.gov.sk*
Mobil: *+421 903 993 706*
Tel: *+421 2 6869 2915*

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

https://access.redhat.com/errata/RHSA-2024:1491
https://access.redhat.com/errata/RHSA-2024:1488
https://access.redhat.com/errata/RHSA-2024:1486
https://access.redhat.com/errata/RHSA-2024:1502
https://access.redhat.com/errata/RHSA-2024:1500
https://access.redhat.com/errata/RHSA-2024:1499
https://access.redhat.com/errata/RHSA-2024:1480
https://access.redhat.com/errata/RHSA-2024:1496
https://access.redhat.com/errata/RHSA-2024:1497

| | | | | | |
|---|---|---|---|---|---|
| **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 bezpečnostné aktualizácie na svoj internetový prehliadač Google, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2024-2883 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webovej stránky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Zneužitie zraniteľnosti vyžaduje interakciu používateľa.
Zneužitím ostatných bezpečnostných zraniteľností možno vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

26.3.2024

## CVE

CVE-2024-1284, CVE-2024-2883, CVE-2024-2885, CVE-2024-2886, CVE-2024-2887

## Zasiahnuté systémy

ChromeOS LTS (Long Term Support) vo verzii staršej ako 114.0.5735.358
Chrome (Android) vo verzii staršej ako 123.0.6312.80
Chrome for Desktop (Windows & Mac) vo verzii staršej ako 123.0.6312.86/87
Chrome for Desktop (Linux) vo verzii staršej ako 122.0.6261.86
Chrome for Desktop (Extended Stable channel) pre Windows a Mac vo verzii staršej ako 122.0.6261.148
ChromeOS/ChromeOS Flex (Beta channel) vo verzii staršej ako 123.0.6312.79

## Následky

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

## Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

## Zdroje

https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_26.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/286320
https://chromereleases.googleblog.com/2024/03/beta-channel-update-for_26.html
https://chromereleases.googleblog.com/2024/03/extended-stable-channel-update-for_26.html
https://chromereleases.googleblog.com/2024/03/chrome-for-android-update_26.html
https://chromereleases.googleblog.com/2024/03/long-term-support-channel-update-for_26.html

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

## Identifikátor

ELECOM WRC wireless routers - tri bezpečnostné zraniteľnosti

## Popis

Spoločnosť ELECOM vydala bezpečnostné aktualizácie na produkty WRC-X3200GST3-B a WRC-G01-W, ktoré opravujú tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2024-25568 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.
Zneužitím ostatných bezpečnostných zraniteľností možno vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

26.3.2024

## CVE

CVE-2024-25568, CVE-2024-26258, CVE-2024-29225

## Zasiahnuté systémy

WRC-X3200GST3-B firmware vo verzii staršej ako Ver.1.27
WRC-G01-W firmware vo verzii staršej ako Ver.1.26

## Následky

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

## Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
SK-CERT administrátorom odporúča venovať osobitnú pozornosť aktualizácii firmvéru, nie len aplikačnému softvéru.

## Zdroje

https://www.elecom.co.jp/news/security/20240326-01/
http://jvn.jp/en/vu/JVNVU95381465/index.html

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

## Identifikátor

Meta Tag Manager WP plugin - bezpečnostná zraniteľnosť

## Popis

Vývojári WordPress pluginu Meta Tag Manager vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-1770 spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom injektovania špeciálne vytvoreného PHP objektu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Ak je v zasiahnutom systéme prítomný POP chain, napríklad prostredníctvom iného nainštalovaného pluginu, možno predmetnú zraniteľnosť zneužiť na odstránenie ľubovoľných súborov v zasiahnutom systéme, neoprávnený prístup k citlivým údajom a vzdialené vykonanie kódu.

## Dátum prvého zverejnenia varovania

27.3.2024

## CVE

CVE-2024-1770

## Zasiahnuté systémy

Meta Tag Manager vo verzii staršej ako 3.1

## Následky

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

## Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky a aplikácie založené na redakčnom systéme WordPress nevyužívajú predmetný plugin v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu redakčného systému a všetkých používaných pluginov na aktuálne verzie bez známych bezpečnostných zraniteľností.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom alebo vzdialené vykonanie kódu, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

## Zdroje

https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/meta-tag-manager/meta-tag-manager-302-authenticated-subscriber-php-object-injection

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

## Identifikátor

Fujidenolo Solutions SonicDICOM Media Viewer - bezpečnostná zraniteľnosť

## Popis

Spoločnosť Fujidenolo Solutions vydala bezpečnostnú aktualizáciu na svoj produkt SonicDICOM Media Viewer, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-29734 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených DLL súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

27.3.2024

## CVE

CVE-2024-29734

## Zasiahnuté systémy

SonicDICOM Media Viewer vo verzii staršej ako (vrátane) 2.3.2

## 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 získanie prístupu k citlivým údajom alebo vzdialené vykonanie kódu, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

## Zdroje

https://jvn.jp/en/jp/JVN40367518/index.html

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

## Identifikátor

Button WP plugin - bezpečnostná zraniteľnosť

## Popis

Bezpečnostní výskumníci zverejnili informácie o bezpečnostnej zraniteľnosti WordPress pluginu Button.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-1872 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom injekcie PHP objektu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

28.3.2024

## CVE

CVE-2024-1872

## Zasiahnuté systémy

Button plugin vo verzii staršej ako 1.1.28 (vrátane)

## Následky

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

## Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné aktualizácie. Odporúčame uistiť sa, či Vaše webové stránky a aplikácie založené na redakčnom systéme WordPress nevyužívajú predmetný plugin v zraniteľnej verzii. V prípade, že áno, administrátorom odporúčame do vydania záplat pluginy v zraniteľných verziách dočasne deaktivovať alebo odinštalovať a vykonať kontrolu integrity redakčného systému.
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.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/button/button-1128-authenticated-contributor-php-object-injection-in-button-shortcode
https://wordpress.org/plugins/button/

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

## Identifikátor

KEYENCE produkty - tri bezpečnostné zraniteľnosti

## Popis

Spoločnosť KEYENCE vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú tri bezpečnostné zraniteľnosti.
Najzávažnejšie bezpečnostné zraniteľnosti s identifikátormi CVE-2024-29218 a CVE-2024-29219 sa nachádzajú v produktoch KV STUDIO a KV REPLAY VIEWER, spočívajú 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. Zneužitie zraniteľnosti vyžaduje interakciu používateľa.

## Dátum prvého zverejnenia varovania

29.3.2024

## CVE

CVE-2024-28099, CVE-2024-29218, CVE-2024-29219

## Zasiahnuté systémy

VT STUDIO vo verzii staršej ako Ver.8.32 (vrátane)
KV STUDIO vo verzii staršej ako Ver.11.64 (vrátane)
KV REPLAY VIEWER vo verzii staršej ako Ver.2.64 (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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

## Zdroje

http://jvn.jp/en/vu/JVNVU92825069/index.html
http://jvn.jp/en/vu/JVNVU95439120/index.html

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

## Identifikátor

RegistrationMagic WP plugin - bezpečnostná zraniteľnosť

## Popis

Vývojári RegistrationMagic pluginu pre WordPress vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-1990 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom SQL injekcie vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

26.3.2024

## CVE

CVE-2024-1990

## Zasiahnuté systémy

RegistrationMagic vo verzii staršej ako 5.3.2.0

## Následky

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

## Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky a aplikácie založené na redakčnom systéme WordPress nevyužívajú predmetný plugin v zraniteľnej verzii. V prípade, že áno, bezodkladne zabezpečte aktualizáciu redakčného systému a všetkých používaných pluginov na aktuálne verzie bez známych bezpečnostných zraniteľností.
Po odstránení zraniteľností, ktoré mohli spôsobiť 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.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/custom-registration-form-builder-with-submission-manager/registrationmagic-custom-registration-forms-user-registration-payment-and-user-login-5310-authenticated-contributor-sql-injection-via-shortcode

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

## Identifikátor

EnvíaloSimple: Email Marketing y Newsletters WP plugin - bezpečnostná zraniteľnosť

## Popis

Bezpečnostní výskumníci zverejnili informácie o bezpečnostnej zraniteľnosti WordPress pluginu EnvíaloSimple: Email Marketing y Newsletters.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-2125 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom CSRF (Cross-Site Request Forgery) útoku uploadovať škodlivé súbory a následne spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti. Zneužitie zraniteľnosti vyžaduje interakciu zo strany používateľa.

## Dátum prvého zverejnenia varovania

1.4.2024

## CVE

CVE-2024-2125

## Zasiahnuté systémy

EnvíaloSimple: Email Marketing y Newsletters vo všetkých verziách

## Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému

## Odporúčania

Na uvedené zraniteľnosti v súčanosti nie sú dostupné aktualizácie. Odporúčame uistiť sa, či Vaše webové stránky a aplikácie založené na redakčnom systéme WordPress nevyužívajú predmetný plugin v zraniteľnej verzii. V prípade, že áno, zabezpečte ich odinštalovanie alebo deaktiváciu a preverte integritu redakčného 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://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/envialosimple-email-marketing-y-newsletters-gratis/envialosimple-email-marketing-y-newsletters-23-cross-site-request-forgery-to-arbitrary-file-upload

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

## Identifikátor

Wireshark - bezpečnostná zraniteľnosť

## Popis

Vývojári open source sieťového analyzátora Wireshark vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2023-6175 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených NetScreen súborov vykonať škodlivý kód a spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému. Zneužitie zraniteľnosti vyžaduje interakciu zo strany používateľa.

## Dátum prvého zverejnenia varovania

28.3.2024

## CVE

CVE-2023-6175

## Zasiahnuté systémy

Wireshark vo verzii staršej ako 4.0.11 a 3.6.19

## Následky

Vykonanie škodlivého kódu a úpné 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 alebo vzdialené vykonanie kódu, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

## Zdroje

https://www.wireshark.org/security/wnpa-sec-2023-29.html
https://www.zerodayinitiative.com/advisories/ZDI-24-355/

**Národný bezpečnostný úrad**
Budatínska 30
851 06 Bratislava

Mail: *sk-cert@nbu.gov.sk*
Mobil: *+421 903 993 706*
Tel: *+421 2 6869 2915*

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

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

## Identifikátor

Microsoft Xbox Gaming Services - bezpečnostná zraniteľnosť

## Popis

Spoločnosť Microsoft vydala bezpečnostnú aktualizáciu na svoj produkt Xbox Gaming Services, 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 eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.
Na uvedenú zraniteľnosť je v súčasnosti voľne dostupný Proof-of-Concept kód.

## Dátum prvého zverejnenia varovania

22.3.2024

## CVE

CVE-2024-28916

## Zasiahnuté systémy

Xbox Gaming Services verzie staršie ako 19.87.13001.0

## Následky

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

## 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://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-28916
https://www.securityweek.com/microsoft-patches-xbox-vulnerability-following-public-disclosure/
https://www.cve.org/CVERecord?id=CVE-2024-28916

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

## Identifikátor

GitLab Community Edition a Enterprise Edition - dve bezpečnostné zraniteľnosti

## Popis

Vývojári platformy GitLab vydali bezpečnostné aktualizácie svojich produktov GitLab Community Edition (CE) a GitLab Enterprise Edition (EE), ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2023-6371 spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom stored cross-site scripting (Stored XSS) útoku vykonať škodlivý kód a následne získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme. Zneužitie zraniteľnosti vyžaduje interakciu zo strany používateľa.
Bezpečnostnú zraniteľnosť s identifikátorom CVE-2024-2818 možno zneužiť na zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

27.3.2024

## CVE

CVE-2023-6371, CVE-2024-2818

## Zasiahnuté systémy

GitLab Community Edition (CE) a GitLab Enterprise Edition (EE) vo verzii staršej ako 16.10.1, 16.9.3, 16.8.5

## Následky

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

## Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom alebo vzdialené vykonanie kódu, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Následne odporúčame preveriť integritu kódu v repozitároch. Odporúčame tiež zaviesť podpisovanie commitov.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

## Zdroje

https://about.gitlab.com/releases/2024/03/27/security-release-gitlab-16-10-1-released/

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

## Identifikátor

Red Hat produkty - viacero bezpečnostných zraniteľností

## Popis

Spoločnosť Red Hat vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2024-25111 sa nachádza v komponente Squid produktu Red Hat Enterprise Linux, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej HTTP požiadavky spôsobiť zneprístupnenie služby.
Zneužitím ostatných bezpečnostných zraniteľností možno vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

26.3.2024

## CVE

CVE-2024-25111, CVE-2024-22019, CVE-2023-46809, CVE-2024-21892, CVE-2023-46137, CVE-2023-46137

## Zasiahnuté systémy

Red Hat Enterprise Linux for ARM 64
Red Hat Enterprise Linux for IBM z Systems
Red Hat Enterprise Linux for Power, little endian
Red Hat Enterprise Linux for x86_64
Red Hat Enterprise Linux Server
Red Hat Enterprise Linux Server for ARM 64
Red Hat Enterprise Linux Server for IBM z Systems
Red Hat Enterprise Linux Server for Power LE
Red Hat OpenStack 16.1 x86_64
Red Hat OpenStack 16.2 x86_64
Red Hat OpenStack Director Deployment Tools 16.1 x86_64
Red Hat OpenStack Director Deployment Tools for IBM Power LE 16.1 ppc64le
Red Hat OpenStack for IBM Power 16.1 ppc64le
Red Hat OpenStack for IBM Power 16.2 ppc64le

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkaze v sekcii ZDROJE

## Následky

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

## Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

## Zdroje

https://access.redhat.com/errata/RHSA-2024:1515
https://access.redhat.com/errata/RHSA-2024:1510
https://access.redhat.com/errata/RHSA-2024:1518
https://access.redhat.com/errata/RHSA-2024:1516

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☐ **Stredná** | ■ **Vysoká** | ☐ **Kritická** | **CVSS skóre:** 8.6 |
| **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 s identifikátorom CVE-2024-20259 sa nachádza v operačnom systéme Cisco IOS XE, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne upravených IPv4 DHCP požiadaviek spôsobiť zneprístupnenie služby.
Ostatné bezpečnostné zraniteľnosti možno zneužiť na neoprávnený prístup k citlivým údajom, neoprávnené zmeny v systéme, zneprístupnenie služby a vzdialené vykonanie škodlivého kódu.

## Dátum prvého zverejnenia varovania

27.3.2024

## CVE

CVE-2024-20259, CVE-2024-20265, CVE-2024-20271, CVE-2024-20276, CVE-2024-20278, CVE-2024-20303, CVE-2024-20306, CVE-2024-20307, CVE-2024-20308, CVE-2024-20309, CVE-2024-20311, CVE-2024-20312, CVE-2024-20313, CVE-2024-20314, CVE-2024-20316, CVE-2024-20324, CVE-2024-20333, CVE-2024-20354

## Zasiahnuté systémy

Catalyst 9000 Series Switches
DNA Traffic Telemetry Appliance
Cisco Wireless LAN Controller
Cisco Catalyst 9800 Series Wireless Controller
Cisco Business Wireless AP
Catalyst 6500 Series Switches with Supervisor Engine 2T or 6T
Catalyst 6800 Series Switches with Supervisor Engine 2T or 6T
Catalyst 9800-CL Wireless Controllers for Cloud
Catalyst 9800 Embedded Wireless Controller for Catalyst 9300, 9400, and 9500 Series Switches
Embedded Wireless Controller on Catalyst APs
Cisco Catalyst Center

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkazoch v sekcii ZDROJE

## Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
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 alebo vzdialené vykonanie kódu, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

## Zdroje

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dhcp-dos-T3CXPO9z
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-secureboot-bypass-zT5vJkSD
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-dos-h9TGGX6W
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dos-Hq4d3tZG
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-priv-esc-seAx6NLX
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-mdns-dos-4hv6pBGf

**Národný bezpečnostný úrad**
Budatínska 30
851 06 Bratislava

Mail: *sk-cert@nbu.gov.sk*
Mobil: *+421 903 993 706*
Tel: *+421 2 6869 2915*

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

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-utd-cmd-JbL8KvHT
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ikev1-NO2ccFWz
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aux-333WBz8f
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-lisp-3gYXs3qP
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-isis-sGjyOUHX
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sda-edge-dos-qZWuWXWG
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dmi-acl-bypass-Xv8FO8Vz
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-wlc-privesc-RjSMrmPK
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ccc-authz-bypass-5EKchJRb
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-airo-ap-dos-PPPtcVW

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☐ **Stredná** | ■ **Vysoká** | ☐ **Kritická** | **CVSS skóre:** 8.2 |
| **Klasifikácia** | ■ **Neutajované / TLP:CLEAR** | | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

NVIDIA ChatRTX - dve bezpečnostné zraniteľnosti

## Popis

Spoločnosť NVIDIA vydala bezpečnostnú aktualizáciu na svoj produkt ChatRTX, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2024-0082 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom podvrhnutia špeciálne vytvorených súborov eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby. Zneužitie zraniteľnosti vyžaduje interakciu používateľa.
Zneužitím druhej bezpečnostnej zraniteľnosti možno vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

26.3.2024

## CVE

CVE-2024-0082, CVE-2024-0083

## Zasiahnuté systémy

ChatRTX vo verzii staršej ako (vrátane) 0.2 - verzia s bezpečnostnou záplatou má názov: ChatWithRTX_installer_3_5.zip

## Následky

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

## Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
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://nvidia.custhelp.com/app/answers/detail/a_id/5532

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

## Identifikátor

Splunk Enterprise - dve bezpečnostné zraniteľnosti

## Popis

Spoločnosť Splunk vydala bezpečnostné aktualizácie na produkty Splunk Enterprise a Splunk Cloud Platform, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2024-29946 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov v komponente Splunk Dashboard Studio a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme. Zneužitie zraniteľnosti vyžaduje interakciu používateľa.
Zneužitím ďalšej bezpečnostnej zraniteľnosti možno získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

27.3.2024

## CVE

CVE-2024-29946, CVE-2024-29945

## Zasiahnuté systémy

Splunk Enterprise vo verzii staršej ako 9.2.1
Splunk Enterprise vo verzii staršej ako 9.1.4
Splunk Enterprise vo verzii staršej ako 9.0.9
Splunk Cloud Platform vo verzii staršej ako 9.1.2312.100

## Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Zneprístupnenie služby

## Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
V prípade, že aktualizácia systému nie je možná, odporúčame postupovať podľa pokynov výrobcu uvedených na odkazoch v sekcii ZDROJE.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

## Zdroje

https://advisory.splunk.com/advisories/SVD-2024-0302
https://advisory.splunk.com/advisories/SVD-2024-0301
https://nvd.nist.gov/vuln/detail/CVE-2024-29946

**Národný bezpečnostný úrad**
Budatínska 30
851 06 Bratislava

Mail: *sk-cert@nbu.gov.sk*
Mobil: *+421 903 993 706*
Tel: *+421 2 6869 2915*

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

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

## Identifikátor

Check & Log Email WP plugin - bezpečnostná zraniteľnosť

## Popis

Vývojári Check & Log Email pluginu pre WordPress vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-0866 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov 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

25.3.2024

## CVE

CVE-2024-0866

## Zasiahnuté systémy

Check & Log Email vo verzii staršej ako 1.0.10

## Následky

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

## Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky a aplikácie založené na redakčnom systéme WordPress nevyužívajú predmetný plugin v zraniteľnej verzii. V prípade, že áno, bezodkladne zabezpečte aktualizáciu redakčného systému a všetkých používaných pluginov na aktuálne verzie bez známych bezpečnostných zraniteľností.
Po odstránení zraniteľností, ktoré mohli spôsobiť 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.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/check-email/check-log-email-109-unauthenticated-hook-injection

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

## Identifikátor

Flexera Software FlexNet Publisher - bezpečnostná zraniteľnosť

## Popis

Spoločnosť Flexera Software vydala bezpečnostnú aktualizáciu na svoj produkt FlexNet Publisher, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-2658 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom podvrhnutia špeciálne vytvorených súborov eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

1.4.2024

## CVE

CVE-2024-2658

## Zasiahnuté systémy

FlexNet Publisher vo verzii staršej ako 2024 R1 (11.19.6.0)

## Následky

Eskalácia privilégií
Vykonanie škodlivého kódu a úplné naručenie 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://community.flexera.com/t5/FlexNet-Publisher-Knowledge-Base/CVE-2024-2658-FlexNet-Publisher-potential-local-privilege/ta-p/313003
https://www.zerodayinitiative.com/advisories/ZDI-24-359/

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☐ **Stredná** | ■ **Vysoká** | ☐ **Kritická** | **CVSS skóre:** 7.7 |
| **Klasifikácia** | ■ **Neutajované / TLP:CLEAR** | | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

Gutenberg Blocks by Kadence Blocks WP plugin - bezpečnostná zraniteľnosť

## Popis

Vývojári Gutenberg Blocks by Kadence Blocks pluginu pre WordPress vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-23500 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom Server-Side Request Forgery (SSRF) útoku získať neoprávnený prístup k citlivým údajom.

## Dátum prvého zverejnenia varovania

25.3.2024

## CVE

CVE-2024-23500

## Zasiahnuté systémy

Gutenberg Blocks by Kadence Blocks vo verzii staršej ako 3.2.20

## Následky

Neoprávnený prístup k citlivým údajom

## Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky a aplikácie založené na redakčnom systéme WordPress nevyužívajú predmetný plugin v zraniteľnej verzii. V prípade, že áno, bezodkladne zabezpečte aktualizáciu redakčného systému a všetkých používaných pluginov na aktuálne verzie bez známych bezpečnostných zraniteľností.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom, 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://nvd.nist.gov/vuln/detail/CVE-2024-23500
https://patchstack.com/database/vulnerability/kadence-blocks/wordpress-kadence-blocks-plugin-3-2-19-server-side-request-forgery-ssrf-vulnerability

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

## Identifikátor

Automation-Direct C-MORE EA9 HMI - tri bezpečnostné zraniteľnosti

## Popis

Spoločnosť Automation Direct vydala bezpečnostnú aktualizáciu na svoj produkt, ktorá opravuje tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2024-25136 spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej URL požiadavky spôsobiť zneprístupnenie služby.
Ostatné bezpečnostné zraniteľnosti možno zneužiť na neoprávnený prístup k citlivým údajom a zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

26.3.2024

## CVE

CVE-2024-25136, CVE-2024-25137, CVE-2024-25138

## Zasiahnuté systémy

C-MORE EA9 HMI EA9-T6CL vo verzii staršej ako 6.78
C-MORE EA9 HMI EA9-T7CL vo verzii staršej ako 6.78
C-MORE EA9 HMI EA0-T7CL-R vo verzii staršej ako 6.78
C-MORE EA9 HMI EA9-T8CL vo verzii staršej ako 6.78
C-MORE EA9 HMI EA9-T10CL vo verzii staršej ako 6.78
C-MORE EA9 HMI EA9-T10WCL vo verzii staršej ako 6.78
C-MORE EA9 HMI EA9-T12CL vo verzii staršej ako 6.78
C-MORE EA9 HMI EA9-T15CL vo verzii staršej ako 6.78
C-MORE EA9 HMI EA9-T15CL-R vo verzii staršej ako 6.78
C-MORE EA9 HMI EA9-RHMI vo verzii staršej ako 6.78
C-MORE EA9 HMI EA9-PGMSW vo verzii staršej ako 6.78

## Následky

Zneprístupnenie služby
Neoprávnený prístup k citlivým údajom

## 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.
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://community.automationdirect.com/s/internal-database-security-advisory/a4GPE0000002oNJ2AY/sa00022
https://community.automationdirect.com/s/internal-database-security-advisory/a4GPE0000002oWz2AI/sa00024
https://community.automationdirect.com/s/internal-database-security-advisory/a4GPE0000002oQX2AY/sa00023

**Národný bezpečnostný úrad**
Budatínska 30
851 06 Bratislava

Mail: *sk-cert@nbu.gov.sk*
Mobil: *+421 903 993 706*
Tel: *+421 2 6869 2915*

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

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

## Identifikátor

Hubbub Lite – Fast, Reliable Social Network Sharing Buttons WP plugin - bezpečnostná zraniteľnosť

## Popis

Vývojári WordPress pluginu Hubbub Lite – Fast, Reliable Social Network Sharing Buttons vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-2501 spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom injektovania špeciálne vytvoreného PHP objektu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Ak je v zasiahnutom systéme prítomný POP chain, napríklad prostredníctvom iného nainštalovaného pluginu, možno predmetnú zraniteľnosť zneužiť na odstránenie ľubovoľných súborov v zasiahnutom systéme, neoprávnený prístup k citlivým údajom a vzdialené vykonanie kódu.

## Dátum prvého zverejnenia varovania

27.3.2024

## CVE

CVE-2024-2501

## Zasiahnuté systémy

Hubbub Lite – Fast, Reliable Social Network Sharing Buttons vo verzii staršej ako 1.33.2

## Následky

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

## Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky a aplikácie založené na redakčnom systéme WordPress nevyužívajú predmetný plugin v zraniteľnej verzii. V prípade, že áno, bezodkladne zabezpečte aktualizáciu redakčného systému a všetkých používaných pluginov na aktuálne verzie bez známych bezpečnostných zraniteľností.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom alebo vzdialené vykonanie kódu, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

## Zdroje

https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/social-pug/hubbub-lite-fast-reliable-social-network-sharing-buttons-1331-php-object-injection

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

## Identifikátor

Wireshark - bezpečnostná zraniteľnosť

## Popis

Vývojári open source aplikácie Wireshark vydali bezpečnostnú aktualizáciu na svoj produkt, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-2955 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky spôsobiť zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

27.3.2024

## CVE

CVE-2024-2955

## Zasiahnuté systémy

Wireshark vo verzii staršej ako 4.2.4 a 4.0.14

## Následky

Zneprístupnenie služby

## Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

## Zdroje

https://www.wireshark.org/security/wnpa-sec-2024-06
https://exchange.xforce.ibmcloud.com/vulnerabilities/286445

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

## Identifikátor

Filter Custom Fields & Taxonomies Light WP plugin - bezpečnostná zraniteľnosť

## Popis

Bezpečnostní výskumníci zverejnili informácie o bezpečnostnej zraniteľnosti WordPress pluginu Filter Custom Fields & Taxonomies Light.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-31094 spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom injekcie špeciálne vytvoreného PHP objektu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

29.3.2024

## CVE

CVE-2024-31094

## Zasiahnuté systémy

Filter Custom Fields & Taxonomies Light vo verzii staršej ako (vrátane) 1.05

## Následky

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

## Odporúčania

Na uvedené zraniteľnosti v súčasnosti nie sú dostupné aktualizácie. Odporúčame uistiť sa, či Vaše webové stránky a aplikácie založené na redakčnom systéme WordPress nevyužívajú predmetný plugin v zraniteľnej verzii. V prípade, že áno, odporúčame do vydania záplat pluginy v zraniteľných verziách dočasne deaktivovať alebo odinštalovať a preveriť integritu redakčného systému.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom alebo vzdialené vykonanie kódu, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

## Zdroje

https://patchstack.com/database/vulnerability/filter-custom-fields-taxonomies-light/wordpress-filter-custom-fields-taxonomies-light-plugin-1-05-php-object-injection-vulnerability

**Národný bezpečnostný úrad**
Budatínska 30
851 06 Bratislava

Mail: *sk-cert@nbu.gov.sk*
Mobil: *+421 903 993 706*
Tel: *+421 2 6869 2915*

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

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

## Identifikátor

SEEnergy SVR-116 - bezpečnostná zraniteľnosť

## Popis

Bezpečnostní výskumníci zverejnili informácie o bezpečnostnej zraniteľnosti produktu Network video recorder SVR-116 od spoločnosti SEEnergy.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-29167 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

27.3.2024

## CVE

CVE-2024-29167

## Zasiahnuté systémy

SVR-116 vo všetkých verziách (ukončená podpora)

## Následky

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

## Odporúčania

Vzhľadom na to, že produkt už nie je udržiavaný, odporúčame prejsť na iný produkt s platnou podporou.
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/JVNVU93932313/index.html

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

## Identifikátor

WP-Members Membership WP plugin - bezpečnostná zraniteľnosť

## Popis

Vývojári WordPress pluginu WP-Members Membership Plugin vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-1852 spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom stored XSS (Cross-Site Scripting) útoku vykonať škodlivý kód a následne získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

## Dátum prvého zverejnenia varovania

1.4.2024

## CVE

CVE-2024-1852

## Zasiahnuté systémy

WP-Members Membership Plugin vo verzii staršej ako 3.4.9.3

## Následky

Vykonanie škodlivého kódu
Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

## Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky a aplikácie založené na redakčnom systéme WordPress nevyužívajú predmetný plugin v zraniteľnej verzii. V prípade, že áno, bezodkladne zabezpečte aktualizáciu redakčného systému a všetkých používaných pluginov na aktuálne verzie bez známych bezpečnostných zraniteľností.
Po odstránení zraniteľností, ktoré mohli spôsobiť 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.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/wp-members/wp-members-membership-plugin-3492-unauthenticated-stored-cross-site-scripting

**Národný bezpečnostný úrad**
Budatínska 30
851 06 Bratislava

Mail: *sk-cert@nbu.gov.sk*
Mobil: *+421 903 993 706*
Tel: *+421 2 6869 2915*

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

# BEZPEČNOSTNÝ BULLETIN

Týždeň 27. 03. 2024 - 02. 04. 2024

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ■ **Stredná** | ☐ **Vysoká** | ☐ **Kritická** | **CVSS skóre:** 6.5 |
| **Klasifikácia** | ■ **Neutajované / TLP:CLEAR** | | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

PI PROFINET - bezpečnostná zraniteľnosť

## Popis

Spoločnosť PI vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť sa nachádza v produktoch PROFINET, spočíva v nedostatočnom overovaní používateľských vstupov v protokole Discovery and Basic Configuration Protocol (DCP) a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente prostredníctvom zaslania špeciálne upravených DCP paketov spôsobiť zneprístupnenie služby.
Bezpečnostná zraniteľnosť nemá pridelený identifikátor CVE.

## Dátum prvého zverejnenia varovania

26.3.2024

## CVE

## Zasiahnuté systémy

Všetky produkty s PROFINET-Specification vo verzii staršej ako 2.4 MU4 [1][2][5]

## 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.
SK-CERT administrátorom odporúča venovať osobitnú pozornosť aktualizácii firmvéru, nie len aplikačnému softvéru.

Výrobca odporúča, tam, kde je to možné, implementovať nasledujúce opatrenia:
- použiť PROFINET Security class 1 alebo vyššiu,
- použiť DCP len v režime na čítanie alebo zakázať používanie DCP v závislosti od prostredia alebo prípadov v ktorých sa používa
- prevádzkovať zraniteľný komponent v stave, v ktorom je DCP automaticky vypnutý
- ak nie je možné deaktivovať používanie DCP, zaistiť prísnu politiku prístupu do siete

Detailné inštrukcie môžete nájsť na webovej adrese uvedenej v sekcii ZDROJE.

## Zdroje

https://www.profibus.com/index.php?eID=dumpFile&t=r&r=62280&dl=1&token=2ff1465e1941b626b0e08045973a7dbda5502149
https://cert-portal.siemens.com/productcert/html/ssb-201698.html