# BEZPEČNOSTNÝ BULLETIN

Týždeň 05. 05. 2021 - 11. 05. 2021

## OBSAH BEZPEČNOSTNÉHO BULLETINU

| Č. | Identifikátor | Dôležitosť | CVSS Skóre |
|---|---|---|---|
| **01.** | Foxit Reader - viacero bezpečnostných zraniteľností | Vysoká | **8.8** |
| **02.** | Delta Electronics CNCSoft ScreenEditor - bezpečnostná zraniteľnosť | Vysoká | **7.8** |
| **03.** | Node.js mixme modul - bezpečnostná zraniteľnosť | Vysoká | **7.5** |
| **04.** | Ruby on Rails - dve bezpečnostné zraniteľnosti | Vysoká | **7.5** |
| **05.** | Trend Micro IM Security produkt - bezpečnostná zraniteľnosť | Vysoká | **7.3** |
| **06.** | EC-CUBE produkt - bezpečnostná zraniteľnosť | Vysoká | **7.1** |

**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**
Naša značka:
01439/2020/SK-CERT-420

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

## Identifikátor

Foxit Reader - viacero bezpečnostných zraniteľností

## Popis

Spoločnosť Foxit vydala bezpečnostnú aktualizáciu na svoj produkt Reader, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených PDF súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

06.05.2021

## CVE

CVE-2021-21822, CVE-2021-31441, CVE-2021-31442, CVE-2021-31454, CVE-2021-31455, CVE-2021-31456, CVE-2021-31457, CVE-2021-31458, CVE-2021-31459, CVE-2021-31460, CVE-2021-31461, CVE-2021-31470, CVE-2021-31472

## Zasiahnuté systémy

Foxit Reader vo verzii staršej ako 10.1.4.37651

## 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.bleepingcomputer.com/news/security/foxit-reader-bug-lets-attackers-run-malicious-code-via-pdfs/
https://www.cybersafe.news/foxit-reader-bug-lets-attackers-run-malicious-code-via-pdfs/
https://talosintelligence.com/vulnerability_reports/TALOS-2021-1287

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

## Identifikátor

Delta Electronics CNCSoft ScreenEditor - bezpečnostná zraniteľnosť

## Popis

Spoločnosť Delta Electronics vydala bezpečnostnú aktualizáciu na svoj produkt CNCSoft ScreenEditor, ktorá opravuje bezpečnostnú zraniteľnosť.

Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby alebo vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

06.05.2021

## CVE

CVE-2021-22672

## Zasiahnuté systémy

Delta Electronics CNCSoft ScreenEditor vo verzii staršej ako 1.01.30

## Následky

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

## Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

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

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://us-cert.cisa.gov/ics/advisories/icsa-21-124-02

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

## Identifikátor

Node.js mixme modul - bezpečnostná zraniteľnosť

## Popis

Vývojári modulu Node.js mixme vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky spôsobiť zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

06.05.2021

## CVE

CVE-2021-29491

## Zasiahnuté systémy

Node.js mixme vo verzii staršej ako 0.5.1

## Následky

Zneprístupnenie služby

## Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie nie sú založené na Node.js mixme v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu komponentov, od ktorých závisí vaša aplikácia, na aktuálne verzie bez známych bezpečnostných zraniteľností.

## Zdroje

https://www.npmjs.com/advisories/1668
https://exchange.xforce.ibmcloud.com/vulnerabilities/201346

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

## Identifikátor

Ruby on Rails - dve bezpečnostné zraniteľnosti

## Popis

Vývojári frameworku Ruby on Rails vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje dve bezpečnostné zraniteľnosti.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej HTTP požiadavky spôsobiť zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

05.05.2021

## CVE

CVE-2021-22902, CVE-2021-22903

## Zasiahnuté systémy

Ruby on Rails vo verzii staršej ako 6.0.3.7
Ruby on Rails vo verzii staršej ako 6.1.0.2

## Následky

Zneprístupnenie služby

## Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie nie sú založené na Ruby on Rails v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu komponentov, od ktorých závisí vaša aplikácia, na aktuálne verzie bez známych bezpečnostných zraniteľností.

## Zdroje

https://seclists.org/oss-sec/2021/q2/99
https://rubyonrails.org/
https://exchange.xforce.ibmcloud.com/vulnerabilities/201281
https://exchange.xforce.ibmcloud.com/vulnerabilities/201282

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

## Identifikátor

Trend Micro IM Security produkt - bezpečnostná zraniteľnosť

## Popis

Spoločnosť Trend Micro vydala bezpečnostnú aktualizáciu na svoj produkt IM Security, ktorá opravuje bezpečnostnú zraniteľnosť.
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

06.05.2021

## CVE

CVE-2021-31520

## Zasiahnuté systémy

IM Security vo verzii staršej ako 1.6.5 CP3 (b2110)
IM Security vo verzii staršej ako 1.6 CP3 (b1267)

## 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 IM Security kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

## Zdroje

https://success.trendmicro.com/solution/000286439
https://exchange.xforce.ibmcloud.com/vulnerabilities/201401
https://www.zerodayinitiative.com/advisories/ZDI-21-525/

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

## Identifikátor

EC-CUBE produkt - bezpečnostná zraniteľnosť

## Popis

Vývojári nástroja EC-CUBE vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej URL získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

10.05.2021

## CVE

CVE-2021-20717

## Zasiahnuté systémy

EC-CUBE vo verzii staršej ako 4.0.5-p1

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

## Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/201497
https://www.ec-cube.net/