# Mesačný prehľad kritických zraniteľností marec 2024

## 1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci marec 2 kritické a 39 vysoko závažných zraniteľnosti.

Kritické zraniteľnosti s označením CVE-2024-21408 a CVE-2024-21407 sa nachádzajú vo virtualizačnej platforme Hyper-V a možno ich zneužiť na zneprístupnenie služby alebo vzdialené vykonanie škodlivého kódu.

Zneužitie zraniteľnosti CVE-2024-21408 vyžaduje nízke oprávnenia a nevyžaduje interakciu používateľa.

Kritická zraniteľnosť CVE-2024-21407 spočíva v použití dealokovaného miesta v pamäti. Na zneužitie tejto zraniteľnosti musí byť útočník prihlásený na hosťovskom systéme a zaslaním špeciálne vytvorených požiadaviek na hardvérové prostriedky dokáže vykonať škodlivý kód na hostiteľskom systéme.

Zraniteľnosti vysokej závažnosti umožňujú vzdialené vykonanie škodlivého kódu, eskaláciu privilégií, zneprístupnenie služby, obchádzanie bezpečnostných prvkov, získanie neoprávneného prístupu k citlivým údajom alebo vykonanie neoprávnených zmien v systéme.

### Zraniteľné systémy:

Windows 10 for 32-bit Systems
Windows 10 for x64-based Systems
Windows 10 Version 1607 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 21H2 for 32-bit Systems
Windows 10 Version 21H2 for ARM64-based Systems
Windows 10 Version 21H2 for x64-based Systems
Windows 10 Version 22H2 for 32-bit Systems
Windows 10 Version 22H2 for ARM64-based Systems
Windows 10 Version 22H2 for x64-based Systems
Windows 11 version 21H2 for ARM64-based Systems
Windows 11 version 21H2 for x64-based Systems
Windows 11 Version 22H2 for ARM64-based Systems
Windows 11 Version 22H2 for x64-based Systems
Windows 11 Version 23H2 for ARM64-based Systems
Windows 11 Version 23H2 for x64-based Systems
Windows Server 2016
Windows Server 2016 (Server Core installation)

Windows Server 2019
Windows Server 2019 (Server Core installation)
Windows Server 2022
Windows Server 2022 (Server Core installation)
Windows Server 2022, 23H2 Edition (Server Core installation)

### Odporúčania:

Odporúčame aplikovať aktualizácie publikované prostredníctvom služby Windows Update. Číslo aktualizácie pre konkrétny systém možno vyhľadať na prvom z nižšie uvedených odkazov vložením identifikátora zraniteľnosti do vyhľadávania.

### Koniec podpory pre Windows Server 2012 a Windows Server 2012 R2

Spoločnosť Microsoft plánovane zrušila podporu pre Windows Server 2012 a Windows Server 2012 R2. Po dátume 10. októbra 2023 už tieto produkty nebudú dostávať aktualizácie zabezpečenia, aktualizácie nesúvisiace so zabezpečením, opravy chýb, technickú podporu a ani aktualizácie technického obsahu online. Odporúčame prejsť na novšiu verziu operačného systému alebo používať rozšírenie ESU na dobu určitú. Viac informácií na stránke.

### Zdroje:

https://msrc.microsoft.com/update-guide/en-us
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21408
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21407
https://www.recordedfuture.com/vulnerability-database/CVE-2024-21408

## 2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft vydala v mesiaci marec bezpečnostné aktualizácie, ktoré opravujú 8 vysoko závažných zraniteľností.

Najzávažnejšie zraniteľnosti s označením CVE-2024-21426 a CVE-2024-21411 sa nachádzajú v produktoch Skype for Consumer a Microsoft SharePoint Server a možno ich zneužiť na vzdialené vykonanie škodlivého kódu.

Zraniteľnosti v produktoch Microsoft Authenticator, Office, Intune Linux Agent a Xbox Gaming Services s označením CVE-2024-21390, CVE-2024-26199, CVE-2024-26201 a CVE-2024-28916 môžu viesť k eskalácii privilégií.

Ostatné vysoko závažné zraniteľnosti možno zneužiť na eskaláciu privilégií a získanie neoprávneho prístupu k citlivým údajom.

### Zraniteľné systémy:

Intune Company Portal for Android
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Authenticator

Microsoft Outlook for Android
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Server 2019
Microsoft SharePoint Server Subscription Edition
Microsoft Teams for Android
Skype for Consumer
Xbox Gaming Services

**Odporúčania:**
Odporúčame aplikovať aktualizácie publikované prostredníctvom služby Windows Update. Číslo aktualizácie pre konkrétny systém možno vyhľadať na prvom z nižšie uvedených odkazov vložením identifikátora zraniteľnosti do vyhľadávania.

**Zdroje:**
https://portal.msrc.microsoft.com/en-us/security-guidance
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21390
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21411
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21426
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21448
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26199
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26201
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26204
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-28916

## 3. Internetové prehliadače

### Microsoft Internet Explorer

Spoločnosť Microsoft ukončila podporu prehliadača Internet Explorer 15.6.2022 pre hlavnú líniu operačných systémov Windows 10 a 11. Spoločnosť Microsoft za mesiac marec neopravila žiadne kritické a vysoko závažné zraniteľnosti pre zvyšné operačné systémy podporujúce Internet Explorer.

**Odporúčania:**
Odporúčame prestať používať a odinštalovať Internet Explorer a nahradiť ho podporovaným prehliadačom Microsoft Edge.

**Zdroje:**
https://msrc.microsoft.com/update-guide/en-us

### Microsoft Edge

Spoločnosť Microsoft v mesiaci marec neopravila v prehliadači Microsoft Edge žiadnu kritickú ani závažnú zraniteľnosť.

### Zdroje:
https://msrc.microsoft.com/update-guide/en-us

## Mozilla Firefox

Spoločnosť Mozilla v mesiaci marec opravila 3 kritické a 7 vysoko závažných zraniteľností v línii internetových prehliadačov Firefox a Firefox ESR.

Kritická zraniteľnosť CVE-2024-2615 (línia Firefox) spočíva v chybách bezpečnosti v pamäti prehliadača, ktoré možno zneužiť na vykonanie ľubovoľného kódu.

CVE-2024-29943 (Firefox) pomocou čítania a zápisu v pamäti mimo povolené hodnoty na JavaScriptovom objekte umožňuje zneprístupnenie služby alebo vykonanie kódu.

Zneužitím zraniteľnosti CVE-2024-29944 (len desktopové verzie Firefox) možno injekciou spracovateľa udalostí do privilegovaného objektu vykonať ľubovoľný JavaScript kód v kontexte rodičovského procesu.

Vysoko závažná zraniteľnosť CVE-2024-2605 (Firefox) umožňuje na zariadeniach s operačným systémom Windows zneužiť Windows Error Reporter na únik zo sandboxu a vykonanie kódu.

CVE-2024-2607 (Firefox) sa týka prepisovania návratových hodnôt registrov na systémoch Armv7-A a umožňuje vykonávanie ľubovoľného kódu.

Zraniteľnosť s označením CVE-2024-2608 (Firefox) súvisí s niektorými funkciami, pri ktorých môže nastať pretečenie celočíselnej premennej a možnosť zapisovať mimo povolené hodnoty v pamäti. by vzdialený neautentifikovaný útočník mohol zneužiť prostredníctvom špeciálne vytvoreného webového obsahu pre vykonanie škodlivého kódu alebo zneprístupnenie služby. Zneužitie zraniteľností si vyžaduje interakciu zo strany používateľa.

Zraniteľnosť CVE-2024-2614 (línie Firefox a Firefox ESR) pokrýva sadu zraniteľností ovplyvňujúcich bezpečnosť pamäte, ktoré môžu viesť ku poškodeniu pamäte alebo možnosti vykonávať kód.

Ostatné zraniteľnosti možno zneužiť na zneprístupnenie služby a obídenie bezpečnostných prvkov.

### Zraniteľné systémy:
Mozilla Firefox verzie staršie ako Firefox 124.0.1
Mozilla Firefox ESR verzie staršej ako 115.9.1

### Odporúčania:
Odporúčame aktualizovať Firefox na verziu 124.0.1 a Firefox ESR na verziu 115.9.1.

### Zdroje:
https://www.mozilla.org/en-US/security/advisories/

https://www.mozilla.org/en-US/security/advisories/mfsa2024-12/
https://www.mozilla.org/en-US/security/advisories/mfsa2024-13/
https://www.mozilla.org/en-US/security/advisories/mfsa2024-15/
https://www.mozilla.org/en-US/security/advisories/mfsa2024-16/
https://exchange.xforce.ibmcloud.com/vulnerabilities/286115
https://exchange.xforce.ibmcloud.com/vulnerabilities/285843

## Google Chrome

V mesiaci marec spoločnosť Google vydala bezpečnostné aktualizácie, ktoré opravili celkom 1 kritickú a 8 vysoko závažných zraniteľností.

Kritická zraniteľnosť s označením CVE-2024-2883 v komponente ANGLE súvisí s možnosťou použitia dealokovaného miesta v pamäti. by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvoreného webového obsahu mohol zneužiť na vykonanie škodlivého kódu a zneprístupnenie služby. Zneužitie zraniteľnosti vyžaduje interakciu zo strany používateľa.

Zraniteľnosti, CVE-2024-2885, CVE-2024-2886, CVE-2024-2400 a CVE-2024-2176 umožňujú zneužiť dealokované miesto v pamäti v komponentoch Dawn, WebCodecs, Performance Manager a FedCM.

Zraniteľnosť CVE-2024-2887 v komponente WebAssembly spočíva v neoverení typu premennej a zraniteľnosť CVE-2024-2625 je chyba životného cyklu objektov v komponente V8.

Zraniteľnosti CVE-2024-2173 a CVE-2024-2174 v komponente V8 súvisia s možnoťou pristupovať k pamäti mimo povolené hodnoty a s bližšie nedefinovanou nevhodnou implementáciou.

Ostatné zraniteľnosti možno zneužiť na obídenie bezpečnostných mechanizmov a získanie neoprávneného prístupu k citlivým údajom.

### Zraniteľné systémy:

Google Chrome pre Windows a Mac verzie staršej ako 123.0.6312.86/.87 a Linux verzie staršej ako 123.0.6312.86.

### Odporúčania:

Odporúčame aktualizáciu prehliadača Chrome pre Windows a Mac verzie staršej ako 123.0.6312.86/.87 a Linux verzie staršej ako 123.0.6312.86.

### Zdroje:

https://chromereleases.googleblog.com/2024/03
https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_26.html
https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_19.html

https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_12.html
https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/286320

## 4. Adobe Acrobat a Reader

V produkte Adobe Acrobat a Reader neboli v mesiaci marec opravené žiadne kritické ani vysoko závažné zraniteľnosti.

**Zdroje:**
https://helpx.adobe.com/security/security-bulletin.html#acrobat

## 5. Frameworky

### Microsoft .NET Framework

V mesiaci marec spoločnosť Microsoft opravila 3 vysoko závažné zraniteľností vo frameworku .NET.

CVE-2024-29059 umožňuje útočníkovi zaslať špeciálne vytvorené požiadavky pre získanie prístupu k citlivým údajom v rámci ObjRef URI.

Zraniteľnosti s označením CVE-2024-26190, CVE-2024-21392 nachádzajúce sa vo frameworku .NET verzie 7.0 a 8.0 by vzdialený neautentifikovaný útočník mohol zneužiť na zneprístupnenie služby.

**Zraniteľné systémy:**
.NET 7.0
.NET 8.0
Microsoft .NET Framework 2.0 Service Pack 2
Microsoft .NET Framework 3.0 Service Pack 2
Microsoft .NET Framework 3.5
Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2
Microsoft .NET Framework 3.5 AND 4.6/4.6.2
Microsoft .NET Framework 3.5 AND 4.7.2
Microsoft .NET Framework 3.5 AND 4.8
Microsoft .NET Framework 3.5 AND 4.8.1
Microsoft .NET Framework 3.5.1
Microsoft .NET Framework 4.6.2
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2
Microsoft .NET Framework 4.8

**Odporúčania:**

Odporúčame aplikovať aktualizácie publikované prostredníctvom služby Windows Update. Číslo aktualizácie pre konkrétny systém možno vyhľadať na prvom z nižšie uvedených odkazov vložením identifikátora zraniteľnosti do vyhľadávania.

**Zdroje:**
https://msrc.microsoft.com/update-guide/en-us
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26190
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21392
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-2905

### Oracle Java

Veľká sada opráv je plánovaná na 16. apríla 2024.

**Zdroje:**
https://www.oracle.com/security-alerts/

## 6. Iné závažné zraniteľnosti

### *Kritická zraniteľnosť v doplnku WordPress*

Obľúbená platforma na tvorbu webových stránok obsahuje kritickú zraniteľnosť typu SQLi, ktorá umožňuje neautentifikovaným útočníkom pripojiť ďalšie dotazy do existujúcich dotazov SQL. To môže viesť k neoprávnenému prístupu k citlivým informáciám. Chyba sa nachádza v populárnom doplnku WordPress s názvom Ultimate Member, ktorý má viac ako 200 000 aktívnych inštalácií. **Viac informácií na stránke.**

### *Kritické zraniteľnosti v produktoch SAP*

Spoločnosť SAP vydala v marci 2024 balík opráv pre svoje produkty opravujúcich 10 zraniteľností v aplikáciách Business Client, Build Apps, NetWeaver AS Java a ďalších. 2 z nich sú označené ako kritické. Úspešné zneužitie umožňuje neautentifikovanému útočníkovi eskaláciu privilégií. **Viac informácií na stránke.**

### *Zraniteľnosti v produktoch NAS*

Spoločnosť QNAP poukázala na bezpečnostné chyby vo svojich softvérových produktoch NAS vrátane QTS, QuTS hero, QuTScloud a myQNAPcloud, ktoré by mohli autentifikovanému útočníkovi umožniť prístup k zariadeniam. Kritické zraniteľnosti umožňujú obídenie autentifikácie, injektovanie príkazov a injekciu SQL. Zraniteľnosti sa nachádzajú na viac ako

3 miliónoch zariadení, ktoré majú prístup na internet. **Viac informácií na stránke.**

## *Kritické zraniteľnosti v produktoch VMware*

Spoločnosť VMware vydala bezpečnostné aktualizácie na opravu kritických zraniteľností úniku zo sandboxu v produktoch VMware ESXi, Workstation, Fusion a Cloud Foundation. Úspešné zneužitie môže viesť k úniku z virtuálnych počítačov a umožniť útočníkom získať prístup k hostiteľskému operačnému systému. **Viac informácií na stránke.**

## *Kritické zraniteľnosti v produktoch Fortinet*

Spoločnosť Fortinet vydala varovanie pred viacerými kritickými a vysoko závažnými zraniteľnosťami v produktoch FortiClientEMS, FortiOS, FortiProxy a FortiManager. Kritické zraniteľnosti umožňujú útočníkovi vykonávanie kódu alebo príkazov prostredníctvom špeciálne vytvorených paketov alebo HTTP požiadaviek. Vysoko závažné zraniteľnosti sa týkajú obchádzania autorizácie a vykonávania ľubovoľného kódu. **Viac informácií na stránke.**

## *Ivanti opravila dve kritické zraniteľnosti*

Spoločnosť Ivanti vydala opravu dvoch kritických zraniteľností, CVE-2023-46808 a CVE-2023-41724, ktoré sa nachádzajú v nástroji Ivanti Standalone Sentry a Ivanti Neurons for ITSM. Úspešné zneužitie umožňuje útočníkovi ľubovoľné vykonávanie príkazov. Chyby boli predmetom zneužitia troch kyberšpionážnych skupín napojených na Čínu. **Viac informácií na stránke.**

## *Kritická zraniteľnosť v serveroch Atlassian*

Atlassian vydal opravy pre viac ako dve desiatky bezpečnostných chýb vrátane kritickej chyby ovplyvňujúcej Bamboo Data Center a Server. Úspešné zneužitie umožňuje injektovanie škodlivých príkazov bez toho, aby bola potrebná interakcia používateľa. **Viac informácií na stránke.**

## *Zero day zraniteľnosti v prehliadači Firefox*

Spoločnosť Mozilla vydala bezpečnostné aktualizácie na opravu dvoch zero-day zraniteľností vo webovom prehliadači Firefox. Zraniteľnosti boli objavené počas hackerskej súťaže Pwn20wn Vancouver 2024. Na obe zraniteľnosti poukázal výskumník Manfred Paul. Viac informácií na stránke.