# Mesačný prehľad kritických zraniteľností
# január 2023

## 1. Operačné systémy Microsoft Windows

Spoločnosť opravila v mesiaci január 11 kritických a 56 vysoko závažných zraniteľností.

Osem kritických zraniteľností umožňuje vzdialené vykonávanie kódu. Zraniteľnosti CVE-2023-21535 a CVE-2023-21548 sa nachádzajú v Secure Socket Tunneling protokole (SSTP). Pre ich zneužitie musí neautentifikovaný útočník vytvoriť špeciálnu požiadavku na pripojenie k RAS serveru alebo špeciálne vytvorený SSTP paket SSTP serveru.

Zraniteľnosti CVE-2023-21543, CVE-2023-21546, CVE-2023-21555, CVE-2023-21556 a CVE-2023-21679 sa nachádzajú v Layer 2 Tunneling protokole (L2TP). Pre ich zneužitie musí neautentifikovaný útočník vytvoriť špeciálnu požiadavku na pripojenie k RAS serveru.

Zraniteľnosť CVE-2023-21712 sa nachádza v Point-to-Point Tunneling protokole. Pre jej zneužitie musí neautentifikovaný útočník vytvoriť špeciálnu požiadavku na pripojenie k RAS serveru.

Ostatné tri kritické zraniteľnosti CVE-2023-21551, CVE-2023-21561 a CVE-2023-21730 umožňujú získať zvýšené privilégiá a nachádzajú sa v Microsoft Cryptographic Services. Úspešné zneužitie umožní útočníkovi získať oprávnenia na úrovní System.

Zraniteľnosti vysokej závažnosti umožňujú vzdialené vykonávanie kódu, obchádzanie zabezpečenia a eskaláciu oprávnení. Zneužitie niektorých z nich môže viesť k úniku informácií a vyvolaniu nedostupnosti služby.

### 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 20H2 for 32-bit Systems
Windows 10 Version 20H2 for ARM64-based Systems
Windows 10 Version 20H2 for x64-based Systems
Windows 10 Version 21H1 for 32-bit Systems
Windows 10 Version 21H1 for ARM64-based Systems
Windows 10 Version 21H1 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 8.1 for 32-bit systems
Windows 8.1 for x64-based systems
Windows RT 8.1
Windows Server 2012
Windows Server 2012 (Server Core installation)
Windows Server 2012 R2
Windows Server 2012 R2 (Server Core installation)
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)

## 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-2023-21535
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21543
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21546
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21548
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21551
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21555
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21556
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21561
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21679
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21712
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21730

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

Spoločnosť opravila v mesiaci január 1 kritickú a 21 vysoko závažných zraniteľností.

Kritická zraniteľnosť CVE-2023-21743 sa nachádza v Microsoft SharePoint Server a umožňuje obchádzať bezpečnostné prvky. Neautentifikovaný útočník dokáže obísť prihlásenie a vytvoriť anonymné spojenie.

Opravené vysoko závažné zraniteľnosti umožňujú vzdialené vykonávanie kódu. Zraniteľnosť CVE-2023-21741 môže byť zneužitá pre získavanie citlivých informácií.

### Zraniteľné systémy:

3D Builder
Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Office 2019 for 32-bit editions
Microsoft Office 2019 for 64-bit editions
Microsoft Office 2019 for Mac
Microsoft Office LTSC 2021 for 32-bit editions
Microsoft Office LTSC 2021 for 64-bit editions
Microsoft Office LTSC for Mac 2021
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Foundation 2013 Service Pack 1
Microsoft SharePoint Server 2019
Microsoft SharePoint Server Subscription Edition
Microsoft Visio 2013 Service Pack 1 (32-bit editions)
Microsoft Visio 2013 Service Pack 1 (64-bit editions)
Microsoft Visio 2016 (32-bit edition)
Microsoft Visio 2016 (64-bit edition)

### 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-2023-21743

# 3. Internetové prehliadače

## Microsoft Internet Explorer

Spoločnosť Microsoft ukončila podporu prehliadača Internet Explorer 15.6.2022 pre hlavnú líniu operačných systémov Windows 10. Pre zvyšné operačné systémy, kde je prehliadač ešte podporovaný, nevydala v mesiaci január žiadne opravy kritických a závažných zraniteľností.

**Zdroje:**
https://portal.msrc.microsoft.com/en-us/security-guidance

## Microsoft Edge

Spoločnosť Microsoft v mesiaci január opravila v prehliadači Microsoft Edge jednu vysoko závažnú zraniteľnosť.

Zraniteľnosť CVE-2023-21795 umožňuje útočníkovi získať vyššie oprávnenia a môže viesť k úniku zo sandboxu prehliadača. Pre jej zneužitie je potrebná interakcia zo strany obete so škodlivým URL odkazom.

**Zraniteľné systémy:**
Microsoft Edge (Chromium-based)

**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-2023-21795

## Mozilla Firefox

V mesiaci január bolo opravených 6 vysoko závažných zraniteľností.

Zraniteľnosť CVE-2023-23597 v produkte Firefox označuje logickú chybu v alokácii procesov, ktorá môže viesť k možnosti čítať ľubovoľný súbor zneužitím detského webového procesu.

Zraniteľnosť CVE-2023-23598 vo verziách Firefox a Firefox ESR pre Linux v komponente Firefox GTK umožňuje zneužiť funkciu drag and drop na prečítanie ľubovoľného súboru pomocou volania „DataTransfer.setData“.

Zraniteľnosť CVE-2023-46871 v produkte Firefox ESR súvisí so zastaranou knižnicou libusrsctp, ktorá obsahuje viaceré zraniteľnosti.

Označenia CVE-2023-23605 (Firefox a Firefox ESR) a CVE-2023-23606 (Firefox) pokrývajú sadu zraniteľností ovplyvňujúcich bezpečnosť pamäte, ktoré môžu viesť ku poškodeniu pamäte alebo možnosti vykonávať kód.

### Zraniteľné systémy:

Mozilla Firefox verzie staršie ako 109

Mozilla Firefox ESR verzie staršej ako 102.7

### Odporúčania:

Odporúčame aktualizáciu Mozilla Firefox na verziu 109 a Mozilla Firefox ESR na verziu 102.7

### Zdroje:

https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-01/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-02/

## Google Chrome

V mesiaci január bola vydaná oprava 4 závažných zraniteľností prehliadača Google Chrome.

CVE-2023-0128, CVE-2023-0471 a CVE-2023-0472 umožňujú použiť dealokované miesto v pamäti v komponentoch Overview Mode, WebTransport a WebRTC.

CVE-2023-0129 súvisí s pretečením medzipamäte na halde v komponente Network Service.

### Zraniteľné systémy:

Google Chrome pre Windows, Mac a Linux verzie staršej ako 109.0.5414.119.

### Odporúčania:

Odporúčame aktualizáciu prehliadača Chrome pre Windows, Mac a Linux aspoň na verziu 109.0.5414.119/.120.

### Zdroje:

https://chromereleases.googleblog.com/2023/01/
https://chromereleases.googleblog.com/2023/01/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2023/01/stable-channel-update-for-desktop_24.html

## 4. Adobe Acrobat a Reader

V produkte Adobe Acrobat a Reader bolo v mesiaci január opravených 11 kritických a 7 vysoko závažných zraniteľností.

Kritické zraniteľnosti CVE-2023-21579, CVE-2023-21604, CVE-2023-21605, CVE-2023-21606, CVE-2023-21607, CVE-2023-21608, CVE-2023-21609, CVE-2023-21610, CVE-2023-22240, CVE-2023-22241 a CVE-2023-22242 umožňujú vykonávanie ľubovoľného kódu kvôli pretečeniu celočíselnej premennej, pretečeniu medzipamäte na halde a zásobníku, chybe zápisu do pamäte mimo povolené hodnoty, nevhodnej validácii vstupov a použitiu dealokovaného miesta v pamäti.

Vysoko závažné zraniteľnosti CVE-2023-21581, CVE-2023-21585, CVE-2023-21613 a CVE-2023-21614 môžu viesť k úniku obsahu pamäte kvôli chybe čítania pamäte mimo povolené hodnoty.

Vysoko závažná zraniteľnosť CVE-2023-21586 môže spôsobiť nedostupnosť aplikácie kvôli chybe dereferencie nulového ukazovateľa.

Vysoko závažné zraniteľnosti CVE-2023-21611 a CVE-2023-21612 môžu viesť k eskalácii privilégií kvôli porušeniu princípov bezpečného dizajnu kódu.

### Zdroje:

https://helpx.adobe.com/security/security-bulletin.html
https://helpx.adobe.com/security/products/acrobat/apsb23-01.html

## 5. Frameworky

## Microsoft .NET Framework

V mesiaci január spoločnosť Microsoft opravila 1 vysoko závažnú zraniteľnosť vo frameworku .NET.

Zraniteľnosť s číslom CVE-2023-21538 môže spôsobiť nedostupnosť služby.

### Zraniteľné systémy:

.NET 6.0

### 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-2023-21538

## Oracle Java

V mesiaci január opravila spoločnosť Oracle v platforme Java SE 1 kritickú zraniteľnosť.

Kritická zraniteľnosť CVE-2022-43548 sa nachádza v komponente Node.js a umožňuje útočníkom vykonávať príkazy v operačnom systéme. Útočník ich môže injektovať vďaka nedostatočnej kontrole parametra „IsIPAddress".

**Zraniteľné systémy:**
Oracle GraalVM Enterprise Edition 20.3.8, 21.3.4 a 22.3.0

**Odporúčania:**
Odporúčame aktualizáciu Oracle GraalVM Enterprise Edition na najnovšiu verziu.

**Zdroje:**
https://www.oracle.com/security-alerts/
https://www.oracle.com/security-alerts/cpujan2023.html#AppendixJAVA
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-43548

# 6. Iné závažné zraniteľnosti

### *Zraniteľnosť v knižnici JSON Web Token umožňuje vykonávať kód*

Tím Auth0 opravil v knižnici JSON Web Token vysoko závažnú zraniteľnosť spojenú s neprítomnosťou kontroly na typ parametru vo funkcii jwt.verify(). Útočníci ju môžu zneužiť pre získanie prístupu k citlivým informáciám alebo možnosti vzdialene vykonávať kód. Viac informácií na stránke.

### *Kritické RCE zraniteľnosti v systéme Git*

V systéme pre riadenie revízií Git boli opravené dve kritické zraniteľnosti vedúce ku pretečeniu medzipamäte na halde. Tretia zraniteľnosť spojená s nedostatočnou kontrolou spúšťaného súboru je hodnotená ako vysoko závažná. Všetky tri umožňujú útočníkom vzdialené vykonávanie kódu. Viac informácií na stránke.

## ***Kritické zraniteľnosti VMware vRealize Log Insight***

Spoločnosť VMware opravila vo svojom nástroji pre zber a analýzu logov vRealize Log Insight dve kritické, jednu vysoko závažnú a jednu stredne závažnú zraniteľnosť. Tieto neautentifikovaným útočníkom umožňujú vzdialene vykonávať kód, spôsobiť nedostupnosť služby a získať citlivé relačné a aplikačné informácie. Viac informácií na stránke.