# Mesačný prehľad kritických zraniteľností
# február 2022

## 1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci február 26 závažných zraniteľností súvisiacich s operačným systémom Windows. Jedenásť zo závažných zraniteľností môže viesť k eskalácii privilégií. Ďalších 9 zraniteľností súvisí so vzdialeným vykonaním kódu. Zneužitím iných 3 zraniteľností môže dôjsť k úniku citlivých informácií. Posledné 3 závažné zraniteľnosti môžu spôsobiť narušenie dostupnosti služby.

**Zraniteľné systémy:**

HEVC Video Extensions
VP9 Video Extensions
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 1909 for 32-bit Systems
Windows 10 Version 1909 for ARM64-based Systems
Windows 10 Version 1909 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 11 for ARM64-based Systems
Windows 11 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)
Windows Server 2022 Azure Edition Core Hotpatch
Windows Server, version 20H2 (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

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

Spoločnosť Microsoft opravila v mesiaci február 11 závažných zraniteľností. Štyri zo závažných zraniteľností (CVE-2022-21988, CVE-2022-22003, CVE-2022-22004 a CVE-2022-22005) umožňujú útočníkom vzdialené vykonávanie kódu. Zraniteľnosti CVE-2022-22716 a CVE-2022-23252 môžu viesť k odhaleniu citlivých informácií. Zneužitím zraniteľnosti CVE-2022-21965 môže dôjsť k narušeniu dostupnosti služby. Zraniteľnosť CVE-2022-21987 môže viesť k umožneniu predstierať cudziu identitu. Posledné tri zraniteľnosti (CVE-2022-21968, CVE-2022-23255 a CVE-2022-23280) môžu viesť k obídeniu bezpečnostných prvkov.

**Zraniteľné systémy:**

Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Excel 2013 RT Service Pack 1
Microsoft Excel 2013 Service Pack 1 (32-bit editions)
Microsoft Excel 2013 Service Pack 1 (64-bit editions)
Microsoft Excel 2016 (32-bit edition)
Microsoft Excel 2016 (64-bit edition)
Microsoft Office 2013 Click-to-Run (C2R) for 32-bit editions
Microsoft Office 2013 Click-to-Run (C2R) for 64-bit editions
Microsoft Office 2013 RT Service Pack 1
Microsoft Office 2013 Service Pack 1 (32-bit editions)
Microsoft Office 2013 Service Pack 1 (64-bit editions)

Microsoft Office 2016 (32-bit edition)
Microsoft Office 2016 (64-bit edition)
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 Office Online Server
Microsoft Office Web Apps Server 2013 Service Pack 1
Microsoft Outlook 2016 for Mac
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 Teams Admin Center
Microsoft Teams for Android
Microsoft Teams for iOS
OneDrive for Android

**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

## 3. Internetové prehliadače

### Microsoft Internet Explorer

Spoločnosť Microsoft neopravila tento mesiac v prehliadači Internet Explorer žiadnu kritickú ani závažnú zraniteľnosť.

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

### Microsoft Edge

Spoločnosť Microsoft opravila tento mesiac v prehliadači Edge 2 závažné zraniteľnosti (CVE-2022-23262 a CVE-2022-23263), ktoré môžu viesť k eskalácii privilégií.

**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

## Mozilla Firefox

V mesiaci február nebola v prehliadači Firefox a Firefox ESR opravená žiadna kritická zraniteľnosť. V prehliadači Firefox boli opravené 4 závažné zraniteľnosti, z čoho 3 sa vyskytujú aj v prehliadači Firefox ESR.

CVE-2022-22753 ovplyvňuje prehliadač pre Windows a súvisí s eskaláciou privilégií na oprávnenia „System“ cez službu Maintenance (Updater).

CVE-2022-22754 sa týka rozšírení. Ak používateľ nainštaloval rozšírenie konkrétneho typu, rozšírenie sa mohlo samo automaticky aktualizovať a počas toho obísť výzvu, ktorá novej verzii udelila nové požadované povolenia.

CVE-2021-22764 vyskytujúca sa v prehliadačoch Firefox 97 a v Firefox ESR 91.6 je séria chýb zabezpečenia v pamäti, z ktorých niektoré majú potenciál zneužitia pre vykonávanie ľubovoľného kódu. CVE-2022-0511 sú tiež chyby pamäte, ale vyskytujúce sa len v prehliadači Firefox 97.

**Zraniteľné systémy:**
Mozilla Firefox verzie staršej ako 97
Mozilla Firefox ESR verzie staršej ako 91.6

**Odporúčania:**
Odporúčame aktualizáciu Firefox na verziu 97 a Firefox ESR na verziu 91.6.

**Zdroje:**
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-04/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-05/

## Google Chrome

V mesiaci február bola vydaná oprava pre 15 závažných zraniteľností.

Závažné zraniteľnosti sa väčšinou týkajú pretečenia medzipamäte haldy, pretečenia celočíselnej premennej, nesprávnej implementácie a použitia odalokovaného miesta v pamäti. Zraniteľnosti sa nachádzajú v komponentoch ako Safe Browsing, ANGLE, V8, GPU, Mojo a ďalších.

**Zraniteľné systémy:**
Google Chrome pre Windows a Linux verzie staršej ako 98.0.4758.102
Google Chrome pre Mac verzie staršej ako 98.0.4758.109

**Odporúčania:**
Odporúčame aktualizáciu prehliadača Chrome pre Windows a Linux na verziu 98.0.4758.102 a pre Mac na verziu 98.0.4758.109.

**Zdroje:**
https://chromereleases.googleblog.com/2022
https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop_14.html
https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop_22.html

## 4. Adobe Acrobat a Reader

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

**Zdroje:**
https://helpx.adobe.com/security.html

## 5. Frameworky

### Microsoft .NET Framework

V mesiaci február spoločnosť Microsoft opravila 1 závažnú zraniteľnosť vo frameworku .NET. Zneužitím zraniteľnosti CVE-2022-21986 môže dôjsť k narušeniu dostupnosti služby.

**Zraniteľné systémy:**

.NET 5.0
.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

### Oracle Java

Veľká sada opráv je plánovaná na 19. apríl 2022.

**Zdroje:**

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

## 6. Iné závažné zraniteľnosti

### *Kritická zraniteľnosť Samba umožňuje vzdialene vykonávať kód*

Populárna implementácia protokolu SMB obsahuje kritickú zraniteľnosť, ktorá umožňuje útočníkom s právami zápisu do súborov vykonávať na diaľku ľubovoľný kód. Spoločnosť Samba zároveň opravila druhú závažnú zraniteľnosť, ktorá môže viesť ku nedostupnosti služby, alebo umožniť útočníkom impersonovať existujúce služby. Viac informácií na stránke.

### *Spoločnosť SAP vydala februárové záplaty – opravuje 19 zraniteľností*

Spoločnosť SAP opravila 19 zraniteľností, pričom CVSS skóre sa pohybuje od 3,7 po 10. Tri kritické zraniteľnosti súvisia s knižnicou Apache Log4j v2. Ďalšie tri zraniteľnosti nazývané ICMAD objavila

spoločnosť Onapsis a ovplyvňujú podnikové aplikácie SAP používajúce ICM (Internet Communication Manager). Viac informácií na stránke.

## ***Závažné zraniteľnosti VMWare produktov***

Spoločnosť VMWare opravila 4 zraniteľnosti týkajúce sa produktov ESXi, Workstation a Fusion, ktoré zneužívajú najmä USB radiče a službu settingsd. Zraniteľnosti sú vysokej závažnosti a ich CVSS skóre sa pohybuje od 8,2 do 8,4. Viac informácií na stránke.