

# Mesačný prehľad kritických zraniteľností

## jún 2021

### 1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci jún 3 kritické a 23 závažných zraniteľností.

Kritická zraniteľnosť CVE-2021-1675 sa vyskytuje v službe Windows Print Spooler. Prvotne bola klasifikovaná ako zraniteľnosť s nízkou závažnosťou umožňujúca eskaláciu privilégií, avšak následne bola prehodnotená ako kritická. Môže viesť k vykonaniu vzdialeného kódu.

Zraniteľnosť CVE-2021-31959 sa nachádza v skriptovacom nástroji a môže viesť k poškodeniu pamäte. Na zneužitie tejto zraniteľnosti je nutná interakcia používateľa. Umožňuje vzdialenému útočníkovi vykonať ľubovoľný kód v cieľovom systéme.

Posledná kritická zraniteľnosť je CVE-2021-33742 a môže viesť k vykonaniu vzdialeného kódu. Nachádza sa v platforme Microsoft MSHTML. Chyba je aktívne zneužívaná a označená za zero-day. Zneužitie vyžaduje interakciu používateľa – útočník musí nalákať používateľa na otvorenie špeciálneho súboru alebo na návštevu škodlivej webovej stránky.

#### 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 1909 for 32-bit Systems  
Windows 10 Version 1909 for ARM64-based Systems  
Windows 10 Version 1909 for x64-based Systems  
Windows 10 Version 2004 for 32-bit Systems  
Windows 10 Version 2004 for ARM64-based Systems  
Windows 10 Version 2004 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 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, version 2004 (Server Core installation)  
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>  
<https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-1675>  
<https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-31959>  
<https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-33742>

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

Spoločnosť Microsoft opravila v mesiaci jún 1 kritickú a 16 závažných zraniteľností. Kritická zraniteľnosť CVE-2021-31963 sa vyskytuje v produkte SharePoint Server a jej zneužitím môže dôjsť k vzdialenému vykonaniu kódu.

Jedenásť zo závažných zraniteľností (CVE-2021-26420, CVE-2021-31939, CVE-2021-31940, CVE-2021-31941, CVE-2021-31942, CVE-2021-31943, CVE-2021-31945, CVE-2021-31946, CVE-2021-31949, CVE-2021-31966 a CVE-2021-31983) umožňuje útočníkom vzdialené vykonávanie kódu. Zneužitie zraniteľností CVE-2021-31948, CVE-2021-31950 a CVE-2021-31964 v produktoch SharePoint môže umožniť predstieranie cudzej identity. Zraniteľnosti CVE-2021-31944 a CVE-2021-31965 môžu viesť k úniku informácií.

### **Zraniteľné systémy:**

3D Viewer  
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 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 Web Apps Server 2013 Service Pack 1  
Microsoft Outlook 2013 RT Service Pack 1  
Microsoft Outlook 2013 Service Pack 1 (32-bit editions)  
Microsoft Outlook 2013 Service Pack 1 (64-bit editions)  
Microsoft Outlook 2016 (32-bit edition)  
Microsoft Outlook 2016 (64-bit edition)  
Microsoft SharePoint Enterprise Server 2013 Service Pack 1  
Microsoft SharePoint Enterprise Server 2016  
Microsoft SharePoint Foundation 2013 Service Pack 1  
Microsoft SharePoint Server 2019  
Office Online Server  
Paint 3D

### **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://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-31963>

## **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 Microsoft Edge 3 závažné zraniteľnosti. Zraniteľnosti CVE-2021-34475 a CVE-2021-33741 môžu viesť k eskalácii privilégií a zneužitím CVE-2021-34506 môže dôjsť k obídeniu bezpečnostných prvkov.

### **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 jún nebola v prehliadači Firefox a Firefox ESR opravená žiadna kritická zraniteľnosť. V prehliadači Firefox boli opravené 2 závažné zraniteľnosti, pričom 1 z nich sa vyskytuje aj v prehliadači Firefox ESR.

Závažná zraniteľnosť CVE-2021-29967 vyskytujúca sa v oboch prehliadačoch môže viesť k poškodeniu pamäte. S dostatočným úsilím by mohol útočník vykonať ľubovoľný kód v cieľovom systéme.

Zraniteľnosť CVE-2021-29965 ovplyvňuje len Firefox pre Android. Škodlivá webová stránka, ktorá vytvára dialógové okno HTTP Authentication by mohla zmiasť vstavaného správcu hesiel. Ten môže navrhnúť heslá pre aktuálne aktívnu webovú stránku namiesto škodlivej stránky, ktorá spustila dialógové okno.

### **Zraniteľné systémy:**

Mozilla Firefox pre Android verzie staršej ako 89.0.1

Mozilla Firefox ESR verzie staršej ako 78.11.

### **Odporúčania:**

Odporúčame aktualizáciu Firefox na verziu 89.0.1 a Firefox ESR na verziu 78.11.

## Zdroje:

<https://www.mozilla.org/en-US/security/advisories/>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2021-23/>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2021-24/>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2021-27/>

## Google Chrome

V mesiaci jún vydala spoločnosť Google opravu pre 1 kritickú a 11 závažných zraniteľností. Kritická zraniteľnosť CVE-2021-30544 sa nachádza v BFCache a týka sa použitia odalokovaného miesta v pamäti. Závažné zraniteľnosti sa väčšinou týkajú použitia odalokovaného miesta v pamäti a zápisu mimo povolených hodnôt. Zraniteľnosti sa nachádzajú v komponentoch WebAudio, WebGL, TabGroups a podobne.

## Zraniteľné systémy:

Google Chrome verzie staršej ako 91.0.4472.123/.124 pre Windows

Google Chrome verzie staršej ako 91.0.4472.114 pre Mac a Linux.

## Odporúčania:

Odporúčame aktualizáciu na verziu 91.0.4472.123/.124 pre Windows a na verziu 91.0.4472.114 pre Mac a Linux.

## Zdroje:

<https://chromereleases.googleblog.com/2021>  
<https://chromereleases.googleblog.com/2021/06/stable-channel-update-for-desktop.html>  
[https://chromereleases.googleblog.com/2021/06/stable-channel-update-for-desktop\\_14.html](https://chromereleases.googleblog.com/2021/06/stable-channel-update-for-desktop_14.html)  
[https://chromereleases.googleblog.com/2021/06/stable-channel-update-for-desktop\\_17.html](https://chromereleases.googleblog.com/2021/06/stable-channel-update-for-desktop_17.html)  
[https://chromereleases.googleblog.com/2021/06/stable-channel-update-for-desktop\\_24.html](https://chromereleases.googleblog.com/2021/06/stable-channel-update-for-desktop_24.html)

## 4. Adobe Flash Player, Acrobat a Reader

V produkte Adobe Acrobat a Reader bolo v júni opravených 5 kritických zraniteľností. Kritické zraniteľnosti CVE-2021-28554 a CVE-2021-28551 súvisia s čítaním mimo povolených hodnôt. CVE-2021-28552, CVE-2021-28631 a CVE-2021-28632 súvisia s použitím odalokovaného miesta v pamäti. Zneužitím sú útočníci schopní vzdialene vykonávať ľubovoľný kód.

Adobe prestala vydávať záplaty pre Flash Player 31. decembra 2020, teda nie je bezpečné ho používať.

### **Zraniteľné systémy:**

Acrobat DC  
Acrobat Reader DC  
Acrobat 2020  
Acrobat Reader 2020  
Acrobat 2017  
Acrobat Reader 2017

### **Odporúčania:**

Odporúčame aktualizáciu:  
Acrobat DC na verziu 2021.005.20048  
Acrobat Reader DC na verziu 2021.005.20048  
Acrobat 2020 na verziu 2020.004.30005  
Acrobat Reader 2020 na verziu 2020.004.30005  
Acrobat 2017 na verziu 2017.011.30197  
Acrobat Reader 2017 na verziu 2017.011.30197

### **Zdroje:**

<https://helpx.adobe.com/security.html>  
<https://helpx.adobe.com/security/products/acrobat/apsb21-37.html>

## **5. Frameworky**

### **Microsoft .NET Framework**

V mesiaci jún spoločnosť Microsoft opravila 1 závažnú zraniteľnosť vo frameworku .NET. Zneužitím CVE-2021-31957 môže dôjsť k narušeniu dostupnosti služby.

### **Zraniteľné systémy:**

.NET 5.0  
.NET Core 3.1

### **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 20. júl 2021.

**Zdroje:**

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