# MESAČNÝ PREHĽAD KRITICKÝCH ZRANITEĽNOSTÍ

OKTÓBER 2024

CSIRT.SK

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

## 1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci október 1 kritickú a 92 vysoko závažných zraniteľností v operačných systémoch Windows.

Kritická zraniteľnosť s označením CVE-2024-43582 sa nachádza v komponente **Remote Desktop Protocol Server** a spočíva v použití odalokovaného miesta v pamäti. Vzdialený neautentifikovaný útočník by ju zaslaním špeciálne vytvorených paketov na špecifické porty mohol zneužiť na vzdialené vykonanie kódu. Zneužitie zraniteľnosti nevyžaduje interakciu zo strany používateľa.

**Microsoft Management Saved Console** obsahuje aktívne zneužívanú zero-day zraniteľnosť, ktorú by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvorených MSC súborov mohol zneužiť na vzdialené vykonanie škodlivého kódu. Zneužitie zraniteľnosti vyžaduje interakciu používateľa, ktorý musí stiahnuť a otvoriť škodlivé súbory. Oprava CVE-2024-43572 zamedzuje otvoreniu MSC súborov z nedôveryhodných zdrojov.

Vysoko závažné zraniteľnosti v komponentoch **Windows Hyper-V** (CVE-2024-30092), **Microsoft OpenSSH for Windows** (CVE-2024-38029, CVE-2024-43581, CVE-2024-43615), **Windows Routing and Remote Access Service** (CVE-2024-38212, CVE-2024-38261, CVE-2024-38265, CVE-2024-43453, CVE-2024-43549, CVE-2024-43564, CVE-2024-43589, CVE-2024-43592, CVE-2024-43593, CVE-2024-43607, CVE-2024-43608, CVE-2024-43611), **Windows Remote Desktop Licensing Service** (CVE-2024-38262), **Microsoft ActiveX Data Objects** (CVE-2024-43517), **Windows Telephony Server** (CVE-2024-43518), **Microsoft WDAC OLE DB provider for SQL** (CVE-2024-43519), **Windows Mobile Broadband Driver** (CVE-2024-43523, CVE-2024-43524, CVE-2024-43525, CVE-2024-43526, CVE-2024-43536, CVE-2024-43543), **Remote Desktop Client** (CVE-2024-43533, CVE-2024-43599), **Windows Shell** (CVE-2024-43552), **Microsoft Speech Application Programming Interface** (CVE-2024-43574) a **utf8asn1str** (CVE-2024-6197) by útočník mohol zneužiť na vzdialené vykonanie kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Ostatné zraniteľnosti vysokej závažnosti možno zneužiť na eskaláciu privilégií, zneprístupnenie služby, obídenie bezpečnostných prvkov, vykonanie neoprávnených zmien v systéme, realizáciu spoofing útokov alebo získanie neoprávneného prístupu k citlivým údajom.

## ZRANITEĽNÉ SYSTÉMY:

- Remote Desktop client for Windows Desktop
- 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 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 10 for 32-bit Systems
- Windows 10 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 11 Version 24H2 for ARM64-based Systems
- Windows 11 Version 24H2 for x64-based Systems
- Windows 11 version 21H2 for ARM64-based Systems
- Windows 11 version 21H2 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.

### ZDROJE:

- https://msrc.microsoft.com/update-guide/en-us
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43582

## 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.

#### ODPORÚČANIA:

Administrátorom a používateľom systémov Windows Server 2012 a Windows Server 2012 R2 odporúčame prejsť na novšiu verziu operačného systému alebo používať rozšírenie ESU na dobu určitú. Viac informácií na stránke.

# 2. KANCELÁRSKE BALÍKY MICROSOFT OFFICE A OFFICE WEB APPS

Spoločnosť Microsoft vydala v mesiaci október bezpečnostné aktualizácie, ktoré opravujú 7 vysoko závažných zraniteľnosti v kancelárskych balíkoch Microsoft Office a Office Web Apps.

CVE-2024-43503 v produkte **Microsoft SharePoint** spočívajú v nesprávnej implementácii mechanizmov riadenia prístupu a lokálny autentifikovaný útočník by ju mohol zneužiť na eskaláciu privilégií na úroveň oprávnenia SYSTEM.

Zraniteľnosti v produktoch **Microsoft Excel** (CVE-2024-43504), **Microsoft Office** (CVE-2024-43616) a **Microsoft Office Visio** (CVE-2024-43505) by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvorených súborov mohol zneužiť na vzdialené vykonanie kódu. Zneužitie zraniteľností vyžaduje interakciu zo strany používateľa, ktorý musí stiahnuť a otvoriť škodlivé súbory.

**Microsoft Office** obsahuje zraniteľnosť CVE-2024-43576, ktorá lokálnemu autentifikovanému útočníkovi umožňuje vykonanie škodlivého kódu.

Zraniteľnosť s identifikátorom CVE-2024-43604 sa nachádza v produkte **Outlook for Android** a vzdialený neautentifikovaný útočník by ju mohol zneužiť na eskaláciu privilégií. Zneužitie zraniteľnosti vyžaduje interakciu zo strany používateľa, ktorý musí otvoriť špeciálne vytvorenú pozvánku na schôdzu alebo udalosť.

CVE-2024-43609 v produkte **Microsoft Office a Microsoft 365** by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvoreného webového obsahu alebo súboru mohol zneužiť na získanie autentifikačných NTLM hashov. Zneužitie zraniteľnosti vyžaduje interakciu zo strany používateľa, ktorý musí kliknúť na URL odkaz alebo otvoriť špeciálne vytvorený súbor. Zneužitie zraniteľnosti je možné mitigovať aj aktiváciou bezpečnostnej politiky pre blokovanie odchádzajúcej NTLM komunikácie na vzdialené servery, pridaním používateľov do skupiny Protected Users Security Group alebo blokovaním odchádzajúcej komunikácie TCP 445/SMB prostredníctvom sieťových alebo bezpečnostných prvkov.

Bližšie nešpecifikovanú zraniteľnosť v produkte **Copilot Studio** (CVE-2024-43610) by vzdialený neautentifikovaný útočník mohol zneužiť na získanie neoprávneného prístupu k citlivým údajom. Zraniteľnosť bola automaticky opravená spoločnosťou Microsoft a nevyžaduje dodatočnú aktualizáciu systémov.

## ZRANITEĽNÉ SYSTÉMY:

- Microsoft 365 Apps for Enterprise for 32-bit Systems
- Microsoft 365 Apps for Enterprise for 64-bit Systems
- Microsoft Copilot Studio
- Microsoft Excel 2016 (32-bit edition)
- Microsoft Excel 2016 (64-bit edition)
- 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 LTSC 2021 for 32-bit editions
- Microsoft Office LTSC 2021 for 64-bit editions
- Microsoft Office LTSC 2024 for 32-bit editions
- Microsoft Office LTSC 2024 for 64-bit editions
- Microsoft Outlook for Android
- Microsoft SharePoint Enterprise Server 2016
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Server Subscription 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-2024-43503
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43504
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43505
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43576

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43604
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43609
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43610
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43616

# 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 október neopravila žiadne kritické ani 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 október opravila 3 vysoko závažné zraniteľnosti vo webovom prehliadači Microsoft Edge.

Zraniteľnosti s označením CVE-2024-43579, CVE-2024-43596 a CVE-2024-43566 spočívajú v nesprávnej manipulácii s dátovými typmi, pretečení medzipamäte haldy a pretečení celočíselnej premennej. Vzdialený neautentifikovaný útočník by ich prostredníctvom podvrhnutia špeciálne vytvoreného webového obsahu mohol zneužiť na vzdialené vykonanie škodlivého kódu. Zneužitie zraniteľností vyžaduje interakciu zo strany používateľa, ktorý musí kliknúť na špeciálne vytvorený URL odkaz.

### ZRANITEĽNÉ SYSTÉMY:

- Microsoft Edge verzie staršie ako 130.0.2849.46
- Microsoft Edge (Chromium-based) verzie staršej ako 130.0.6723.59

### ODPORÚČANIA:

Odporúčame aktualizovať Microsoft Edge aspoň na verziu 130.0.2849.46 a Chromium-based na verziu 130.0.6723.59.

### ZDROJE:

- https://msrc.microsoft.com/update-guide/en-us
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43579
- https://exchange.xforce.ibmcloud.com/vulnerabilities/382699
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43596
- https://exchange.xforce.ibmcloud.com/vulnerabilities/382704
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43566
- https://exchange.xforce.ibmcloud.com/vulnerabilities/382698

## MOZILLA FIREFOX

Spoločnosť Mozilla v mesiaci október opravila 1 kritickú a 10 vysoko závažných zraniteľností v línii internetových prehliadačov Firefox a Firefox ESR.

Kritická zero-day zraniteľnosť CVE-2024-9680 (línia Firefox a Firefox ESR) v rozhraní AnimationTimeline spočíva v použití odalokovaného miesta v pamäti a možno ju zneužiť na vzdialené vykonanie kódu. AnimationTimeline je súčasťou Firefox Web Animations API a slúži na kontrolu a synchronizáciu animovaných prvkov na webstránkach. Zraniteľnosť je aktívne zneužívaná útočníkmi.

Zraniteľnosti CVE-2024-9401, CVE-2024-9402 (Firefox, Firefox ESR) a CVE-2024-9403 (línia Firefox) predstavujú bezpečnostné chyby pamäte a vzdialený neautentifikovaný útočník by ich mohol zneužiť na vzdialené vykonanie škodlivého kódu alebo zneprístupnenie služby.

CVE-2024-10459 (Firefox, Firefox ESR) a CVE-2024-9936 (línia Firefox) spočívajúce v použití odalokovaného miesta v pamäti a chybnej implementácii cache možno zneužiť na zneprístupnenie služby.

Obe línie prehliadačov obsahujú zraniteľnosti, ktoré možno zneužiť na obídenie bezpečnostných prvkov prehliadača (CVE-2024-10458, CVE-2024-9392) a získanie neoprávneného prístupu k citlivým údajom z cross-origin obsahu vo formáte JSON a PDF (CVE-2024-9393, CVE-2024-9394).

Mozilla Firefox for Android obsahuje zraniteľnosť CVE-2024-9391, ktorá pri otvorení špeciálne vytvoreného webového obsahu v režime zobrazenia na celú obrazovku zabraňuje opusteniu tohto zobrazenia a má za následok zmiznutie poľa pre zadávanie URL adries.

Zneužitie všetkých zraniteľností vyžaduje interakciu zo strany používateľa, ktorý musí otvoriť špeciálne vytvorený webový obsah.

## ZRANITEĽNÉ SYSTÉMY:

- Mozilla Firefox verzie staršie ako 132
- Mozilla Firefox ESR verzie staršej ako 128.4

## ODPORÚČANIA:

Odporúčame aktualizovať Firefox na verziu 132 a Firefox ESR na verziu 128.4.

## ZDROJE:

- https://www.mozilla.org/en-US/security/advisories/
- https://www.mozilla.org/en-US/security/advisories/mfsa2024-57/
- https://www.mozilla.org/en-US/security/advisories/mfsa2024-56/
- https://www.mozilla.org/en-US/security/advisories/mfsa2024-55/
- https://www.mozilla.org/en-US/security/advisories/mfsa2024-53/
- https://www.mozilla.org/en-US/security/advisories/mfsa2024-51/
- https://www.mozilla.org/en-US/security/advisories/mfsa2024-48/
- https://www.mozilla.org/en-US/security/advisories/mfsa2024-47/
- https://www.mozilla.org/en-US/security/advisories/mfsa2024-46/
- https://exchange.xforce.ibmcloud.com/vulnerabilities/380476
- https://exchange.xforce.ibmcloud.com/vulnerabilities/380499
- https://exchange.xforce.ibmcloud.com/vulnerabilities/380500
- https://exchange.xforce.ibmcloud.com/vulnerabilities/380501

- https://exchange.xforce.ibmcloud.com/vulnerabilities/380508
- https://exchange.xforce.ibmcloud.com/vulnerabilities/380509
- https://exchange.xforce.ibmcloud.com/vulnerabilities/380510
- https://exchange.xforce.ibmcloud.com/vulnerabilities/381568
- https://exchange.xforce.ibmcloud.com/vulnerabilities/382068
- https://exchange.xforce.ibmcloud.com/vulnerabilities/385417
- https://exchange.xforce.ibmcloud.com/vulnerabilities/385419

## GOOGLE CHROME

V mesiaci október spoločnosť Google vydala bezpečnostné aktualizácie, ktoré opravili 1 kritickú a 10 vysoko závažných zraniteľností.

Kritická zraniteľnosť CVE-2024-10487 v komponente Dawn spočíva v čítaní mimo povolených hodnôt a vzdialený neautentifikovaný útočník by ju mohol zneužiť na vykonanie škodlivého kódu.

Komponenty Extensions (CVE-2024-10229), V8 (CVE-2024-9370) a Mojo (CVE-2024-9369) obsahujú zraniteľnosti, ktoré možno zneužiť na obídenie bezpečnostných prvkov prehliadača.

Pretečenie celočíselnej premennej v rámci komponentu Layout (CVE-2024-7025), nesprávne vyhodnocovanie dátových typov vo V8 (CVE-2024-10230, CVE-2024-10231, CVE-2024-9602, CVE-2024-9603) a použitie odalokovaného miesta v pamäti v komponentoch WebRTC (CVE-2024-10488) a AI (CVE-2024-9954) by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvoreného webového obsahu mohol zneužiť na vykonanie škodlivého kódu.

Zneužitie všetkých vyššie uvedených zraniteľností vyžaduje interakciu zo strany používateľa, ktorý musí otvoriť špeciálne vytvorený webový obsah.

### ZRANITEĽNÉ SYSTÉMY:

- Google Chrome pre Windows a Mac verzie staršej ako 130.0.6723.91/.92
- Google Chrome pre Linux verzie staršej ako 130.0.6723.91

### ODPORÚČANIA:

Odporúčame aktualizáciu prehliadača Chrome pre Windows a Mac aspoň na verziu 130.0.6723.91/.92 a Linux verzie aspoň na verziu 130.0.6723.91.

### ZDROJE:

- https://chromereleases.googleblog.com/2024
- https://chromereleases.googleblog.com/2024/10/stable-channel-update-for-desktop_29.html
- https://chromereleases.googleblog.com/2024/10/stable-channel-update-for-desktop_22.html
- https://chromereleases.googleblog.com/2024/10/stable-channel-update-for-desktop_15.html
- https://chromereleases.googleblog.com/2024/10/stable-channel-update-for-desktop_8.html
- https://chromereleases.googleblog.com/2024/10/stable-channel-update-for-desktop.html
- https://exchange.xforce.ibmcloud.com/vulnerabilities/385536
- https://exchange.xforce.ibmcloud.com/vulnerabilities/383420
- https://exchange.xforce.ibmcloud.com/vulnerabilities/380474
- https://exchange.xforce.ibmcloud.com/vulnerabilities/383418
- https://exchange.xforce.ibmcloud.com/vulnerabilities/383419
- https://exchange.xforce.ibmcloud.com/vulnerabilities/381422
- https://exchange.xforce.ibmcloud.com/vulnerabilities/381421
- https://exchange.xforce.ibmcloud.com/vulnerabilities/385538
- https://exchange.xforce.ibmcloud.com/vulnerabilities/382393
- https://exchange.xforce.ibmcloud.com/vulnerabilities/380472
- https://exchange.xforce.ibmcloud.com/vulnerabilities/380473

## 4. ADOBE ACROBAT A READER

V mesiaci október spoločnosť Adobe neopravila žiadne kritické ani vysoko závažné zraniteľnosti v produktoch Adobe Acrobat a Reader.

### ZDROJE:

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

# 5. FRAMEWORKY

## MICROSOFT .NET FRAMEWORK

V mesiaci október spoločnosť Microsoft opravila 4 vysoko závažné zraniteľnosti vo frameworku .NET.

CVE-2024-38229 v produktoch .NET a Visual Studio spočíva v použití odalokovaného miesta v pamäti, ktoré možno zneužiť na vzdialené vykonanie škodlivého kódu. Pre úspešné zneužitie zraniteľnosti musí útočník vyhrať súbeh procesov.

Zraniteľnosti s označením CVE-2024-43483, CVE-2024-43484 (.NET, .NET Framework, Visual Studio) a CVE-2024-43485 (.NET, Visual Studio) spočívajú v neefektívnej implementácii bližšie nešpecifikovaných algoritmov a vzdialený neautentifikovaný útočník by ich prostredníctvom zaslania špeciálne vytvorených požiadaviek mohol zneužiť na zneprístupnenie služby.

### ZRANITEĽNÉ SYSTÉMY:

- .NET 6.0 installed on Linux
- .NET 6.0 installed on Mac OS
- .NET 6.0 installed on Windows
- .NET 8.0 installed on Linux
- .NET 8.0 installed on Mac OS
- .NET 8.0 installed on Windows
- 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 4.7.2
- 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 4.6/4.6.2
- 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 vyhľadávača.

### ZDROJE:

- https://msrc.microsoft.com/update-guide/en-us
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38229
- https://exchange.xforce.ibmcloud.com/vulnerabilities/381338
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43483
- https://exchange.xforce.ibmcloud.com/vulnerabilities/381347
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43484
- https://exchange.xforce.ibmcloud.com/vulnerabilities/381348
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43485
- https://exchange.xforce.ibmcloud.com/vulnerabilities/381349

## ORACLE JAVA

Spoločnosť Oracle v mesiaci október vydala bezpečnostné aktualizácie, ktoré opravujú 3 vysoko závažné zraniteľnosti v rámci Oracle Java SE.

Oracle GraalVM for JDK obsahuje zraniteľnosť CVE-2024-36138, ktorá sa nachádza v externom komponente Node.js a vzdialený neautentifikovaný útočník by ju mohol zneužiť na získanie úplnej kontroly nad zraniteľnou inštanciou GraalVM for JDK.

Zraniteľnosti s označením CVE-2023-42950 a CVE-2024-25062 (Oracle Java SE, Oracle GraalVM Enterprise Edition) sa nachádzajú v komponentoch JavaFX (WebKitGTK) a JavaFX(libxml2) a vzdialený neautentifikovaný útočník by ju mohol zneužiť na zneprístupnenie služby alebo získanie úplnej kontroly nad zraniteľnou inštanciou Oracle Java SE alebo Oracle GraalVM Enterprise Edition. Zneužitie zraniteľnosti CVE-2023-42950 vyžaduje interakciu zo strany používateľa.

### ZRANITEĽNÉ SYSTÉMY:

- Oracle GraalVM for JDK: 17.0.12, 21.0.4, 23
- Oracle Java SE: 8u421
- Oracle GraalVM Enterprise Edition: 20.3.15, 21.3.1

### ODPORÚČANIA:

Odporúčame aktualizovať zraniteľné verzie Java SE na aktuálne verzie prostredníctvom Java Auto Update alebo na stránke spoločnosti Oracle, ktorú môžete nájsť v časti zdroje.

### ZDROJE:

- https://www.oracle.com/security-alerts/
- https://www.oracle.com/security-alerts/cpuoct2024.html
- https://www.oracle.com/security-alerts/cpuoct2024verbose.html#JAVA

## 6. INÉ ZÁVAŽNÉ ZRANITEĽNOSTI

### PROTECT AI: OKTÓBROVÉ ZRANITEĽNOSTI V MODELOCH AI

Protect AI's huntr je prvý program odmeňovania za nájdenie zraniteľností v oblasti AI/ML na svete. Októbrová správa tejto iniciatívy informuje o 34 objavených zraniteľnostiach v nástrojoch, z toho sú 3 kritické. Najzávažnejšie chyby umožňujú vzdialené vykonávanie kódu, prístup ku chráneným zdrojom a únik citlivých informácií. Viac informácií na stránke.

### KRITICKÁ ZRANITEĽNOSŤ SPRING WEBFLUX

Spoločnosť Broadcom vydala bezpečnostné aktualizácie, ktoré opravujú kritickú bezpečnostnú zraniteľnosť vo webovom frameworku Spring WebFlux. Bližšie nešpecifikovanú zraniteľnosť s označením CVE-2024-38821 by vzdialený neautentifikovaný útočník mohol zneužiť na obídenie bezpečnostných mechanizmov a narušenie dôvernosti a integrity systému. Viac informácií na stránke.

### KRITICKÁ ZRANITEĽNOSŤ V PRODUKTOCH QNAP HBS 3 HYBRID BACKUP SYNC A SMB SERVICE

Spoločnosť QNAP vydala bezpečnostné aktualizácie svojho nástroja pre zálohovanie a obnovu dát HBS 3 (HYBRID BACKUP SYNC), ktoré opravujú kritickú zero-day zraniteľnosť. CVE-2024-50388 možno zneužiť na vzdialené vykonanie kódu. HBS 3 je používaný v rámci sieťových úložísk QNAP NAS s operačnými systémami QTS a QuTS hero. Aktualizácie opravujú tiež kritickú zero-day zraniteľnosť SMB Service, ktorá umožňuje útoky typu SQL injection a získanie kontroly nad zariadením. Viac informácií na stránke.

## NVIDIA OPRAVILA ZÁVAŽNÉ ZRANITEĽNOSTI OVLÁDAČOV

Spoločnosť nVidia vydala bezpečnostné aktualizácie, ktoré opravujú viacero vysoko závažných zraniteľností v ovládačoch grafických kariet. Najzávažnejšiu zraniteľnosť s označením CVE-2024-0126 by lokálny autentifikovaný útočník mohol zneužiť na eskaláciu privilégií a vykonanie škodlivého kódu. Ostatné zraniteľnosti možno zneužiť na vykonanie kódu, zneprístupnenie služby, eskaláciu privilégií a získanie neoprávneného prístupu k citlivým údajom. Viac informácií na stránke.

## KRITICKÉ ZRANITEĽNOSTI PRODUKTOV CISCO

Spoločnosť Cisco opravila kritické zraniteľnosti vo viacerých svojich produktoch. Zraniteľnosti Cisco Secure Firewall Management Center a Adaptive Security Appliance umožňujú vykonávanie ľubovoľných systémových príkazov s oprávneniami používateľa root. Zraniteľnosť Firepower Threat Defense súvisí s prítomnosťou prihlasovacích údajov v kóde systému a umožňuje tak neoprávnený prístup do systému. Viac informácií na stránke.

## NOVÚ KRITICKÚ ZRANITEĽNOSŤ FORTIMANAGER AKTÍVNE ZNEUŽÍVAJÚ NA VYKONÁVANIE KÓDU

Spoločnosť Fortinet opravila kritickú aktívne zneužívanú zero-day zraniteľnosť v produkte FortiManager. CVE-2024-47575 spočíva v chýbajúcej autentifikácii pre prístup ku rozhraniu API, ktoré umožňuje vykonávanie príkazov, prístup k citlivým údajom a prevzatie kontroly nad FortiManager a v ňom spravovanými zariadeniami. Viac informácií na stránke.

## POTENCIÁLNA ZRANITEĽNOSŤ FRAMEWORKU NETTE UMOŽŇUJÚCA SQL INJECTION

Bezpečnostní analytici CSIRT.SK objavili potenciálnu zraniteľnosť vo webovom frameworku Nette, ktorá umožňuje vykonávať útoky typu SQL injection. Zraniteľnosť sa nachádza v knižnici Database a súvisí s absenciou ošetrovania používateľských vstupov, ktoré preberá funkcia where($by). Viac informácií na stránke.

## ZÁVAŽNÁ ZRANITEĽNOSŤ WINDOWS REGISTRY

Microsoft opravil vysoko závažnú zraniteľnosť vo Windows Registry, ktorá umožňuje eskaláciu oprávnení na serveri na úroveň SYSTEM. Zraniteľnosť bola opravená v rámci októbrového balíka Microsoft Patch Tuesday. Viac informácií na stránke.

## ZRANITEĽNOSTI F5 BIG-IP A BIG-IQ

Spoločnosť F5 vydala bezpečnostné aktualizácie, ktoré opravujú 2 zraniteľnosti v F5 BIG-IP a F5 BIG-IQ. Vzdialený autentifikovaný útočník ich dokáže zneužiť na zvýšenie privilégií, vykonávanie kódu JavaScript a prevzatie kontroly nad zariadením. Viac informácií na stránke.

## VYSOKO ZÁVAŽNÁ ZRANITEĽNOSŤ V PRODUKTE VMWARE HCX

Spoločnosť BROADCOM vydala bezpečnostné aktualizácie, ktoré opravujú vysoko závažnú zraniteľnosť v produkte VMware HCX. CVE-2024-38814 možno prostredníctvom SQL injekcie zneužiť na vzdialené vykonanie kódu. Viac informácií na stránke.

## KRITICKÁ ZRANITEĽNOSŤ V PRODUKTE TREND MICRO CLOUD EDGE

Spoločnosť Trend Micro vydala bezpečnostné aktualizácie, ktoré opravujú kritickú zraniteľnosť v produkte Cloud Edge. Zraniteľnosť o označením CVE-2024-48904 možno zneužiť na vzdialené vykonanie škodlivého kódu. Viac informácií na stránke.

## KRITICKÁ ZRANITEĽNOSŤ GITLAB UMOŽŇUJE ĽUBOVOĽNÉ SPUSTENIE CI/CD PIPELINOV

Spoločnosť GitLab vydala aktualizáciu, ktorá opravuje osem zraniteľností. Najzávažnejšie umožňujú vzdialeným útočníkom spustiť CI/CD pipeline na ľubovoľnej vetve repozitára a vykonávať škodlivý kód. Medzi ďalšie závažné zraniteľnosti patrí možnosť realizácie SSRF a XSS útokov, zneprístupnenie služieb a neoprávnený prístup k citlivým údajom. Viac informácií na stránke.

## MICROSOFT PATCH TUESDAY OPRAVUJE 5 ZERO-DAY ZRANITEĽNOSTÍ

Spoločnosť Microsoft v rámci októbrového Patch Tuesday vydala bezpečnostné aktualizácie svojich produktov, ktoré opravujú 118 zraniteľností, z toho 3 kritické, 5 zero-day a 2 aktívne zneužívané. Zero-day zraniteľnosti umožňujú vzdialené vykonanie kódu, obídenie bezpečnostných prvkov, eskaláciu privilégií a realizáciu útokov falšovaním rôznych prvkov. Viac informácií na stránke.

## KRITICKÉ ZRANITEĽNOSTI PALO ALTO NETWORKS EXPEDITION

Spoločnosť Palo Alto Networks vydala bezpečnostné aktualizácie, ktoré opravujú viacero zraniteľností v produkte Expedition. Zraniteľnosti možno zneužiť na SQL injekciu, realizáciu XSS útokov, získanie neoprávneného prístupu k citlivým údajom a čítanie a zápis ľubovoľných súborov na súborovom systéme Expedition. Útočníci môžu získať schopnosť vzdialene vykonať

škodlivý kód a získať úplnú kontrolu nad firewallmi s operačným systémom PAN-OS. Viac informácií na stránke.

## AKTÍVNE ZNEUŽÍVANÁ RCE ZRANITEĽNOSŤ FIREFOX

Spoločnosť Mozilla opravila vo svojom prehliadači kritickú aktívne zneužívanú zraniteľnosť. Jej zneužitím získajú útočníci možnosť vzdialene vykonávať kód. Viac informácií na stránke.

## KRITICKÉ A ZERO-DAY ZRANITEĽNOSTI ČIPOV QUALCOMM

Spoločnosť QUALCOMM vydala bezpečnostné aktualizácie, ktoré opravujú aktívne zneužívanú zero-day zraniteľnosť v službe DSP (Digital Signal Processor) využívanej vo viacerých chipsetoch a kritickú zraniteľnosť v komponente WLAN Resource Manager. Viac informácií na stránke.

## ZRANITEĽNOSŤ APACHE AVRO UMOŽŇUJE VYKONÁVAŤ KÓD

Systém pre serializáciu dát Apache Avro Java SDK kvôli chybe v spracovaní používateľských schém umožňuje útočníkom získať schopnosť vzdialeného vykonávania kódu. Viac informácií na stránke.

## ZRANITEĽNOSŤ WORDPRESS LITESPEED CACHE UMOŽŇUJE STORED XSS

Vývojári pluginu WordPress LiteSpeed Cache vydali bezpečnostné aktualizácie, ktoré opravujú vysoko závažnú zraniteľnosť súvisiacu s absentujúcou sanitizáciou parametrov z HTTP požiadaviek. Tieto plugin preberá a ukladá na administrátorskú stránku, čo vedie k možnosti vykonávať útoky typu stored XSS. Viac informácií na stránke.

## KRITICKÉ ZRANITEĽNOSTI V IDS/IPS SURICATA

Vývojári IDS/IPS systému a sieťového analyzátora Suricata vydali aktualizáciu svojho produktu, ktorá opravuje šesť zraniteľností, z čoho tri sú označené ako kritické. Zraniteľnosti možno zneužiť na obídenie bezpečnostných mechanizmov, vzdialené vykonanie škodlivého kódu a zneprístupnenie služby. Viac informácií na stránke.