Mesačný prehľad kritických zraniteľností
január 2024

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci január 2 kritické a 38 vysoko závažných zraniteľností.

Kritická zraniteľnosť CVE-2024-20674 sa nachádza v kryptografickom komponente Kerberos a umožňuje obísť bezpečnostné prvky. Úspešné zneužitie umožňuje útočníkom vydávať sa za systém Windows, keď používateľ pripojí klienta systému Windows k škodlivému serveru.

Zraniteľnosť CVE-2024-20700 sa nachádza vo virtualizačnej platforme Hyper-V a umožňuje vzdialené vykonávanie kódu. Úspešné zneužitie tejto zraniteľnosti si vyžaduje, aby útočník zneužil súbeh a pred spustením útoku najprv získal prístup do obmedzenej siete.

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

Zraniteľné systémy:

Raw Image Extension
Remote Desktop client for Windows Desktop
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 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 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-2024-20674
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20700

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť opravila v mesiaci január 2 vysoko závažné zraniteľnosti.

Vysoko závažná zraniteľnosť CVE-2024-20677 sa nachádza v súborovom formáte FBX a môže viesť k vzdialenému vykonávaniu kódu.

Zraniteľnosť CVE-2024-21318 umožňuje autentifikovanému útočníkovi v role Site Owner vykonať kód na diaľku na serveri SharePoint. Úspešné zneužitie umožňuje útočníkovi injektovať a vykonať škodlivý kód.

Zraniteľné systémy:

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 Publisher 2013 Service Pack 1 (32-bit editions)
Microsoft Publisher 2013 Service Pack 1 (64-bit editions)

Microsoft Publisher 2013 Service Pack 1 RT
Microsoft Publisher 2016 (32-bit edition)
Microsoft Publisher 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
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-2024-20677
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21318

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. Pre zvyšné operačné systémy, kde je prehliadač ešte podporovaný, nevydala v mesiaci január žiadne opravy kritických a závažných zraniteľností.

Odporúčania:

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

Zdroje:

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

Microsoft Edge

Spoločnosť Microsoft v mesiaci január opravila v prehliadači Microsoft Edge 3 vysoko závažné zraniteľnosti.

Vysoko závažné zraniteľnosti CVE-2024-21326, CVE-2024-21385 a CVE-2024-21388 môžu viesť k eskalácii oprávnení.

Pre úspešné zneužitie zraniteľnosti CVE-2024-21326 je potrebné aby obeť klika na útočníkom podvrhnutý odkaz. To by mohlo viesť k úplnej kompromitácii prehliadača.

Zraniteľnosti CVE-2024-21385 a CVE-2024-21388 môžu viesť k úniku zo sandboxu prehliadača. Úspešné zneužitie si vyžaduje od útočníka vykonanie dodatočných krokov pred samotným zneužitím na prípravu cieľového prostredia.

Zraniteľné systémy:

Microsoft Edge (Chromium-based) build 120.0.6099.268, 120.0.6099.276, 121.0.6167.85/.86 a 121.0.6167.139/140

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-2024-21326
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21385
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21388

Mozilla Firefox

V mesiaci január bolo opravených 5 vysoko závažných zraniteľností v línii Firefox a Firefox ESR.

Vysoko závažná zraniteľnosť CVE-2024-0741 sa nachádza v komponente ANGLE (Almost Native Graphics Layer Engine) a týka sa zapisovania mimo povolené hodnoty pamäte.

Zraniteľnosť CVE-2024-0742 sa týka nesprávnej aktualizácie časovej pečiatky vstupu používateľa.

Chyba CVE-2024-0743 (Firefox) sa nachádza v knižniciach Network Security Services (NSS) a týka sa absencie kontroly návratovej hodnoty v kóde TLS handshake, čo môže vyvolať nedostupnosť služby.

CVE-2024-0744 (Firefox) súvisí s chybou dereferencie divokého ukazovateľa v kóde kompilovanom v JIT a môže spôsobiť nedostupnosť aplikácie.

Chyba CVE-2024-0745 (Firefox) súvisí s pretečením zásobníka na halde v komponente WebAudio a môže viesť k nedostupnosti aplikácie.

Zraniteľné systémy:

Mozilla Firefox verzie staršie ako Firefox 122
Mozilla Firefox ESR verzie staršej ako 115.7

Odporúčania:

Odporúčame aktualizáciu Mozilla Firefox na verziu 122 a Mozilla Firefox ESR na verziu 115.7.

Zdroje:

https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2024-01/
https://www.mozilla.org/en-US/security/advisories/mfsa2024-02/

Google Chrome

V mesiaci január bola vydaná oprava 14 vysoko závažných zraniteľností prehliadača Google Chrome.

Vysoko závažné zraniteľnosti CVE-2024-0222, CVE-2024-0224, CVE-2024-0225, CVE-2024-0807, CVE-2024-1077, CVE-2024-1059 a CVE-2024-1060 umožňujú použiť dealokované miesto v pamäti v komponentoch ANGLE, WebAudio, WebGPU, Network, WebRTC a Canvas.

Zraniteľnosť CVE-2024-0812 sa týka nevhodnej implementácie v komponente Accessibility.

Chyba CVE-2024-0808 je zraniteľnosť súvisiaca s pretečením celočíselnej premennej v komponente WebUI.

CVE-2024-0517, CVE-2024-0518 a CVE-2024-0519 sa nachádzajú v komponente V8. Zraniteľnosti sa týkajú zapisovania a pristupovania do pamäte mimo povolené hodnoty a neoverenia typu premennej.

CVE-2024-0333 súvisí s nedostatočným overením nedôveryhodných vstupov v komponente Extensions.

CVE-2024-0223 sa týka pretečenia medzipamäte na halde v komponente ANGLE.

Zraniteľné systémy:

Google Chrome pre Windows verzie staršej ako 121.0.6167.139/140 a Linux a Mac verzie staršej ako 121.0.6167.139.

Odporúčania:

Odporúčame aktualizáciu prehliadača Chrome pre Windows aspoň na verziu 121.0.6167.139/140 a Linux a Mac aspoň na verziu 121.0.6167.139.

Zdroje:

https://chromereleases.googleblog.com/2024/01
https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_30.html
https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html
https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_16.html
https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_9.html
https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop.html

4. Adobe Acrobat a Reader

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

Zdroje:

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

5. Frameworky

Microsoft .NET Framework

V mesiaci január spoločnosť Microsoft opravila 5 vysoko závažných zraniteľností vo frameworku .NET.

Vysoko závažná zraniteľnosť CVE-2024-0056 sa nachádza v Microsoft.Data.SqlClient a System.Data.SqlClient SQL Data Provider a týka sa obchádzania bezpečnostných prvkov.

CVE-2024-0057 sa nachádza vo frameworku .NET, NET a Visual Studio a týka sa obchádzanie bezpečnostných prvkov.

Zraniteľnosti CVE-2024-20672, CVE-2024-21312 a CVE-2024-21319 sa nachádzajú vo frameworku .NET a Microsoft Identity. Úspešné zneužitie môže viesť k vyvolaniu nedostupnosti služby.

Zraniteľné systémy:

Microsoft .NET Framework 2.0 Service Pack 2
Microsoft .NET Framework 3.5 AND 4.8.1
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2
Microsoft .NET Framework 3.5 AND 4.7.2
Microsoft .NET Framework 3.5 AND 4.8
Microsoft .NET Framework 4.8
Microsoft .NET Framework 3.5
Microsoft .NET Framework 3.0 Service Pack 2
.NET 8.0
.NET 7.0
.NET 6.0

Zdroje:

https://portal.msrc.microsoft.com/en-us/security-guidance
https://nvd.nist.gov/vuln/detail/CVE-2024-0056
https://nvd.nist.gov/vuln/detail/CVE-2024-0057
https://nvd.nist.gov/vuln/detail/CVE-2024-20672
https://nvd.nist.gov/vuln/detail/CVE-2024-21312
https://nvd.nist.gov/vuln/detail/CVE-2024-21319

Oracle Java

V mesiaci január opravila spoločnosť Oracle v platforme Java SE a GraalVM Enterprise Edition 5 vysoko závažných zraniteľností.

Zraniteľnosť CVE-2023-44487 sa nachádza v protokole HTTP/2 a umožňuje vyvolanie odopretia služby.

Chyba CVE-2023-5072 sa nachádza v analyzátore a úspešné zneužitie môže viesť k odmietnutiu služby vo verziách JSON-Java do 20230618 vrátane.

Zraniteľnosti CVE-2024-20932, CVE-2024-20952 a CVE-2024-20918 umožňujú neautentifikovanému útočníkovi vytvoriť, vymazať, upraviť citlivé údaje alebo inak kompromitovať systém. Pre úspešné zneužitie musí mať útočník prístup do siete.

Zraniteľné systémy:

Oracle Java SE: 17.0.9, 8u391, 8u391-perf, 11.0.21, 17.0.9, 21.0.1; Oracle GraalVM for JDK: 17.0.9, 21.0.1; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8, 22.3.4

Odporúčania:

Odporúčame aktualizáciu Oracle JavaSE a GraalVM Enterprise Edition na najnovšiu verziu.

Zdroje:

https://www.oracle.com/security-alerts/
https://www.oracle.com/security-alerts/cpujan2024.html
https://nvd.nist.gov/vuln/detail/CVE-2023-44487
https://nvd.nist.gov/vuln/detail/CVE-2023-5072
https://nvd.nist.gov/vuln/detail/CVE-2024-20918
https://nvd.nist.gov/vuln/detail/CVE-2024-20932
https://nvd.nist.gov/vuln/detail/CVE-2024-20952

6. Iné závažné zraniteľnosti

Zero-day zraniteľnosť v Google Chrome

Google vydal neočakávanú bezpečnostnú aktualizáciu pre aktívne zneužívanú zero-day zraniteľnosť. Zraniteľnosť CVE-2024-0519 je aktívne zneužívaná a môže viesť k vzdialenému vykonávaniu kódu. **Viac informácií na stránke.**

Kritická zraniteľnosť v Confluence Data Center a Server

Spoločnosť Atlassian vydala bezpečnostnú opravu pre kritickú zraniteľnosť CVE-2023-22527, ktorá umožňuje vzdialené vykonávanie kódu na koncových zariadeniach. **Viac informácií na stránke.**

Aktívne zneužívaná zraniteľnosť v BIG-IP

Spoločnosť F5 poukázala na aktívne zneužívanú zraniteľnosť CVE-2023-46747, ktorá umožňuje neautentifikovanému útočníkovi vzdialené vykonávanie kódu. Existuje viac ako 6 000 internetových inštancií, ktoré používajú aplikačnú sieťovú bezpečnosť BIG-IP, ktoré sú potenciálne ohrozené. **Viac informácií na stránke.**

Dve zero-day zraniteľnosti v produktoch Ivanti

Spoločnosť Ivanti poukázala na dve aktívne zneužívané zero-day zraniteľnosti v produktoch Ivanti. Zraniteľnosti sú aktívne zneužívané a boli zneužité hackerskou skupinou napojenou na čínsku vládu. **Viac informácií na stránke.**

Aktívne zneužívaná zraniteľnosť v serveri SharePoint

Spoločnosť CISA vydala varovanie pre aktívne zneužívanú zraniteľnosť CVE-2023-29357 v Microsoft SharePoint Server. Spoločnosť Microsoft vydala záplaty na túto chybu v rámci júnových aktualizácií 2023 Patch Tuesday. **Viac informácií na stránke.**

Zraniteľnosť vo FortiOS a FortiProxy

Google vydal neočakávanú bezpečnostnú aktualizáciu pre aktívne zneužívanú zero-day zraniteľnosť. Zraniteľnosť CVE-2024-0519 je aktívne zneužívaná a môže viesť k vzdialenému vykonávaniu kódu. **Viac informácií na stránke.**