Mesačný prehľad kritických zraniteľností december 2022

1. Operačné systémy Microsoft Windows

Spoločnosť opravila v mesiaci december 3 kritické a 23 vysoko závažných zraniteľností.

Všetky tri opravené kritické zraniteľnosti umožňujú vzdialené vykonávanie kódu. Zraniteľnosť CVE-2022-41076 sa nachádza v prostredí PowerShell. Prihlásený útočník ju môže zneužiť na únik z PowerShell Remoting Session Configuration a vykonávanie príkazov na zraniteľnom systéme. Zraniteľnosti CVE-2022-44670 a CVE-2022-44676 sa nachádzajú v protokole SSTP. Pre ich zneužitie musí neautentifikovaný útočník vytvoriť špeciálnu požiadavku na pripojenie k RAS serveru.

Zraniteľnosti vysokej závažnosti umožňujú vzdialené vykonávanie kódu 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-2022-41076
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44670
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44676

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť opravila v mesiaci december 2 kritické a 14 vysoko závažných zraniteľností.

Kritické zraniteľnosti CVE-2022-44690 a CVE-2022-44693 sa nachádzajú v Microsoft SharePoint Server a umožňujú vzdialené vykonávanie kódu. Zneužiť ich dokáže autentifikovaný útočník s oprávneniami Manage List.

Opravené vysoko závažné zraniteľnosti CVE-2022-44702, CVE-2022-47211, CVE-2022-47212, CVE-2022-47213, CVE-2022-26804, CVE-2022-26805, CVE-2022-26806, CVE-2022-44691, CVE-2022-44692, CVE-2022-44694, CVE-2022-44695, CVE-2022-44696 umožňujú vzdialené vykonávanie kódu. Zraniteľnosť CVE-2022-44713 umožňuje predstierať cudziu identitu a CVE-2022-24480 dovoľuje získať vyššie oprávnenia.

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 Outlook for Android
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)
Windows Terminal for Windows 10
Windows Terminal for Windows 11

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-2022-44690
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44693

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 december žiadne opravy kritických a závažných zraniteľností.

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

Microsoft Edge

Spoločnosť Microsoft v mesiaci december opravila v prehliadači Microsoft Edge jednu kritickú zraniteľnosť.

Zraniteľnosť CVE-2022-44708 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-2022-44708

Mozilla Firefox

V mesiaci december bolo opravených 6 vysoko závažných zraniteľností.

Zraniteľnosť CVE-2022-46871 v produkte Firefox označuje implementovanú zastaranú verziu knižnice libusrsctp, ktorá obsahuje nešpecifikované zraniteľnosti.

Zraniteľnosť CVE-2022-46872 vo verziách Firefox a Firefox ESR pre Linux dovoľuje útočníkovi čítať ľubovoľné súbory pomocou správ IPC.

CVE-2022-46880 v produkte Firefox ESR umožňuje použitie dealokovaného miesta v pamäti v komponente WebGL.

CVE-2022-46881 vo Firefox ESR súvisí s nesprávnou optimalizáciou v komponente WebGL a vedie k porušeniu pamäte.

Označenia CVE-2022-46878 (Firefox a Firefox ESR) a CVE-2022-46879 (Firefox) pokrývajú sadu zraniteľností ovplyvňujúcich bezpečnosť pamäte, ktoré môžu viesť ku poškodeniu pamäte alebo možnosti vykonávať kód.

Zraniteľné systémy:
Mozilla Firefox verzie staršie ako 108
Mozilla Firefox ESR verzie staršej ako 102.6

Odporúčania:
Odporúčame aktualizáciu Mozilla Firefox na verziu 108 a Mozilla Firefox ESR na verziu 102.6

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-51/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-52/

Google Chrome
V mesiaci december bola vydaná oprava 6 závažných zraniteľností prehliadača Google Chrome.

CVE-2022-4436, CVE-2022-4437, CVE-2022-4438, CVE-2022-4439 a CVE-2022-4440 umožňujú použiť dealokované miesto v pamäti v komponentoch Blink Media, Mojo IPC, Blink Frames, Aura a Profiles.

CVE-2022-4262 súvisí s neoverením typu premennej v komponente V8. Zraniteľnosť je aktívne zneužívaná.

Zraniteľné systémy:
Google Chrome pre Windows, Mac a Linux verzie staršej ako 106.0.5249.91.

Odporúčania:
Odporúčame aktualizáciu prehliadača Chrome pre Windows, Mac a Linux aspoň na verziu 108.0.5359.124/.125.

Zdroje:
https://chromereleases.googleblog.com/2022/12/
https://chromereleases.googleblog.com/2022/12/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2022/12/stable-channel-update-for-desktop_13.html

4. Adobe Acrobat a Reader

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

Zdroje:

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

5. Frameworky

Microsoft .NET Framework

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

Zraniteľnosť s číslom CVE-2022-41089 umožňuje vzdialené vykonávanie kódu.

Zraniteľné systémy:

.NET 6.0
.NET 7.0
.NET Core 3.1
Microsoft .NET Framework 2.0 Service Pack 2
Microsoft .NET Framework 3.0 Service Pack 2
Microsoft .NET Framework 3.5 / 3.5.1
Microsoft .NET Framework 4.6 / 4.6.2
Microsoft .NET Framework 4.7 / 4.7.1 / 4.7.2
Microsoft .NET Framework 4.8 / 4.8.1

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
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41089

Oracle Java

Veľká sada opráv je plánovaná na 17. január 2023.

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

6. Iné závažné zraniteľnosti

Oprávnenia root vďaka trojkombinácii zraniteľností v Ubuntu Linux

Tím Ubuntu opravil vo viacerých podporovaných verziách tejto distribúcie Linuxu vysoko závažnú zraniteľnosť v nástroji Snapd. V kombinácii so zraniteľnosťami označenými ako Leeloo Multipath umožňuje lokálnemu útočníkovi bez oprávnení získať oprávnenia používateľa root. Útočník môže získať tiež schopnosť vykonávať ľubovoľný kód. Viac informácií na stránke.

Závažné zraniteľnosti FortiOS a FortiProxy

Spoločnosť Fortinet vydala opravné aktualizácie pre FortiOS a FortiProxy, odstraňujúce kritickú zero-day zraniteľnosť umožňujúcu vzdialené vykonávanie kódu a vysoko závažnú zraniteľnosť poskytujúcu útočníkom možnosť obchádzať autentifikáciu. Viac informácií na stránke.

Zraniteľnosť Foxit PDF Reader a Foxit PDF Editor umožňuje vzdialene vykonávať kód

Spoločnosť Foxit opravila v produktoch Foxit PDF Reader a PDF Editor (PhantomPDF) kritickú zraniteľnosť, ktorá umožňuje útočníkom vzdialene vykonávať kód. Viac informácií na stránke.