Mesačný prehľad kritických zraniteľností september 2022

1. Operačné systémy Microsoft Windows

Spoločnosť opravila v mesiaci september 3 kritické a 45 vysoko závažných zraniteľností.

Všetky tri opravené kritické zraniteľnosti umožňujú vzdialené vykonávanie kódu. Kritická zraniteľnosť CVE-2022-34718 ovplyvňuje implementáciu protokolu TCP/IP, zraniteľnosti CVE-2022-34721 a CVE-2022-34722 sa nachádzajú v protokole Windows Internet Key Exchange (IKE). Pre ich zneužitie môže útočník odoslať zraniteľnému zariadeniu špeciálne vytvorený IP paket.

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

Zraniteľné systémy:

AV1 Video Extension
Raw Image Extension
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 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

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-2022-34718
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34721
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34722

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť opravila v mesiaci september 7 vysoko závažných zraniteľností.

Opravené zraniteľnosti CVE-2022-35823, CVE-2022-37961, CVE-2022-37962, CVE-2022-37963, CVE-2022-38008, CVE-2022-38009, CVE-2022-38010 umožňujú vzdialené vykonávanie kódu. Nachádzajú sa v produktoch Microsoft Visio, Sharepoint a balíkoch Office.

Zraniteľné systémy:

Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
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 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)
SharePoint Server Subscription Edition Language Pack

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 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 september žiadne opravy kritických a závažných zraniteľností.

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

Microsoft Edge

Spoločnosť Microsoft v mesiaci september neopravila v prehliadači Microsoft Edge žiadnu kritickú ani vysoko závažnú zraniteľnosť.

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

Mozilla Firefox

V mesiaci september boli opravené 4 vysoko závažné zraniteľnosti.

Zraniteľnosť CVE-2022-3266 umožňuje čítanie mimo povolených hodnôt v pamäti pri dekódovaní videoformátu H264.

Zraniteľnosť CVE-2022-40959 umožňuje získať oprávnenia zariadenia pre nedôveryhodné dokumenty obídením obmedzení FeaturePolicy.

CVE-2022-40960 môže dovoliť použitie dealokovaného miesta v pamäti keď URL parser spracováva URL, ktoré nie sú vo formáte UTF-8.

Označenie CVE-2022-40962 pokrýva sadu zraniteľností ovplyvňujúcich bezpečnosť pamäte, ktoré môžu viesť ku poškodeniu pamäte alebo možnosti vykonávať kód.

Zraniteľné systémy:

Mozilla Firefox verzie staršie ako 105
Mozilla Firefox ESR verzie staršej ako 102.3

Odporúčania:

Odporúčame aktualizáciu Mozilla Firefox na verziu 105 a Mozilla Firefox ESR na verziu 102.3

Zdroje:

https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-40/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-41/

Google Chrome

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

Zraniteľnosť CVE-2022-3075 súvisí s nedostatočnou validáciou dát v komponente Mojo.

CVE-2022-3195 a CVE-2022-3373 umožňujú zapisovať do pamäte mimo povolených hodnôt v komponente Storage a V8.

CVE-2022-3196, CVE-2022-3197, CVE-2022-3198, CVE-2022-3199, CVE-2022-3304, CVE-2022-3305, CVE-2022-3306, CVE-2022-3307 a CVE-2022-3370 umožňujú použiť dealokované miesto v pamäti v komponentoch PDF, Frames, CSS, Survey, Media a Custom Elements.

CVE-2022-3200 je chyba pretečenia medzipamäte haldy v komponente Internals.

CVE-2022-3201 súvisí s nedostatočným overením nedôveryhodných vstupov v komponente DevTools.

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 106.0.5249.91.

Zdroje:

https://chromereleases.googleblog.com/2022/09/
https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_14.html
https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_27.html
https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_30.html

4. Adobe Acrobat a Reader

V produkte Adobe Acrobat a Reader boli v mesiaci september opravené 3 kritické a 4 vysoko závažné zraniteľnosti.

Kritické zraniteľnosti CVE-2022-35665, CVE-2022-35666 a CVE-2022-35667 umožňujú útočníkom vykonávať ľubovoľný kód kvôli chybám zápisu na dealokované miesto v pamäti, nevhodnej kontrole vstupov a zápisu mimo povolený rozsah v pamäti.

Vysoko závažné zraniteľnosti CVE-2022-35668, CVE-2022-35670, CVE-2022-35671 a CVE-2022-35678 môžu viesť k úniku obsahu pamäte kvôli chybám zápisu na dealokované miesto v pamäti, nevhodnej kontrole vstupov a čítania mimo povolený rozsah v pamäti.

Zraniteľné systémy:

Acrobat DC 22.001.20169 a staršie
Acrobat Reader DC 22.001.20169 a staršie
Acrobat 2020 20.005.30362 a staršie
Acrobat Reader 2020 20.005.30362 a staršie
Acrobat 2017 17.012.30249 a staršie
Acrobat 2017 17.012.30249 a staršie

Odporúčania:

Odporúčame aktualizáciu na verziu:

Acrobat DC 22.002.20191
Acrobat Reader DC 22.002.20191
Acrobat 2020 20.005.30381
Acrobat Reader 2020 20.005.30381
Acrobat 2017 17.012.30262
Acrobat 2017 17.012.30262

Zdroje:

https://helpx.adobe.com/security.html
https://helpx.adobe.com/security/products/acrobat/apsb22-39.html

5. Frameworky

Microsoft .NET Framework

V mesiaci september spoločnosť Microsoft opravila 2 závažné zraniteľnosti vo frameworku .NET.

Zraniteľnosť s číslom CVE-2022-26929 umožňuje vzdialené vykonávanie kódu a CVE-2022-38013 môže viesť k vyvolaniu nedostupnosti služby.

Zraniteľné systémy:

.NET 6.0
.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
Microsoft .NET Framework 3.5 AND 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 3.5 AND 4.8.1
Microsoft .NET Framework 3.5.1
Microsoft .NET Framework 4.6
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2
Microsoft .NET Framework 4.8
Microsoft .NET Framework 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-2022-26929
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38013

Oracle Java

Veľká sada opráv je plánovaná na 18. október 2022.

Zdroje:
https://www.oracle.com/technetwork/topics/security/alerts-086861.html

6. Iné závažné zraniteľnosti

Kritická zneužívaná zraniteľnosť Sophos Firewall

Kritická zero-day zraniteľnosť v Sophos Firewall umožňuje útočníkom vzdialene vykonávať kód. Spoločnosť Sophos vydala opravu pre podporované verzie svojho produktu. Viac informácií na stránke.

Microsoft v rámci Patch Tuesday opravil závažnú aktívne zneužívanú zraniteľnosť vo Windows

Spoločnosť Microsoft vydala v septembri 2022 balík opráv pre operačné systémy Windows opravujúcich 63 zraniteľností. 5 z nich dostalo hodnotenie kritická. Dve zraniteľnosti sú typu zero-day, pričom jedna je aktívne zneužívaná. Viac informácií na stránke.

Závažná zraniteľnosť v HP Support Assistant

Spoločnosť HP opravila závažnú zraniteľnosť v nástroji HP Support Assistant, ktorá umožňuje

útočníkom eskalovať privilégiá škodlivého kódu na úroveň SYSTEM. Viac informácií na stránke.

Kritické zraniteľnosti sieťových dátových úložísk QNAP a Zyxel

Spoločnosť QNAP opravila nešpecifikovanú kritickú zraniteľnosť vo svojom produkte Photo Station pre úložiská NAS, ktorú aktívne zneužíva skupina Deadbolt vo svojej ransomvérovej kampani. Spoločnosť Zyxel opravila vo firmvéri svojich zariadení NAS kritickú zraniteľnosť umožňujúcu jednoduchým spôsobom vzdialené vykonávanie kódu. Viac informácií na stránke.