Mesačný prehľad kritických zraniteľností
október 2022

1. Operačné systémy Microsoft Windows

Spoločnosť opravila v mesiaci október 10 kritických a 57 vysoko závažných zraniteľností.

Sedem opravených kritických zraniteľností umožňuje vzdialené vykonávanie kódu. Nachádzajú sa v protokole Point-to-Point a majú označenia CVE-2022-22035, CVE-2022-30198, CVE-2022-33634, CVE-2022-24504, CVE-2022-41081, CVE-2022-38000, CVE-2022-38047.

Dve z kritických zraniteľností umožňujú zvýšenie oprávnení. CVE-2022-37976 sa nachádza v v certifikačnej službe Active Directory, CVE-2022-37979 bola nájdená vo virtualizačnej platforme Hyper-V.

Posledná opravená kritická zraniteľnosť CVE-2022-34689 umožňuje predsteiranie cudzej identity a nachádza sa v komponente.

Zraniteľnosti vysokej závažnosti umožňujú vzdialené vykonávanie kódu, eskaláciu oprávnení a obídenie bezpečnostných prvkov. Zneužitie niektorých z nich môže viesť k úniku informácií, možnosti predstierať cudziu identitu, či 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 11 for ARM64-based Systems
Windows 11 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-2022-22035
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24504
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30198
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-33634
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38000
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38047
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41081
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37976
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37979
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34689

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť opravila v mesiaci október 2 kritické a 7 vysoko závažných zraniteľností.

Kritické zraniteľnosti CVE-2022-38048 a CVE-2022-41038, ktoré sa nachádzajú v Microsoft Office a SharePoint Server, umožňujú vzdialené vykonávanie kódu.

Päť z vysoko závažných zraniteľností CVE-2022-38049, CVE-2022-38053, CVE-2022-41031, CVE-2022-41036, CVE-2022-41037 umožňuje vzdialené vykonávanie kódu. Nachádzajú sa v Microsoft Office a SharePoint Server.

Vysoko závažná zraniteľnosť CVE-2022-38001 v Microsoft Office umožňuje predstierať cudziu identitu a CVE-2022-41043 môže viesť k úniku citlivých informácií.

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

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-2022-38048
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38049
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38053
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41031
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41036
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41037
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41038

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38001
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41043

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 október žiadne opravy kritických a závažných zraniteľností.

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

Microsoft Edge

Spoločnosť Microsoft v mesiaci október 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 október boli opravené 2 vysoko závažné zraniteľnosti.

Zraniteľnosť CVE-2022-42927 môže viesť k úniku záznamov prístupov k URL na iných doménach cez funkciu performance.getEntries(). Umožňuje to porušenie same-origin politiky.

Zraniteľnosť CVE-2022-42928 v JS Engine môže viesť k poškodeniu pamäte. Súvisí to s chýbajúcimi anotáciami pri určitých typoch alokácií.

Zraniteľné systémy:
Mozilla Firefox verzie staršie ako 106
Mozilla Firefox ESR verzie staršej ako 102.4

Odporúčania:
Odporúčame aktualizáciu Mozilla Firefox na verziu 106 a Mozilla Firefox ESR na verziu 102.4

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

https://www.mozilla.org/en-US/security/advisories/mfsa2022-44/

Google Chrome

V mesiaci október bola vydaná oprava 10 závažných zraniteľností prehliadača Google Chrome.

Zraniteľnosti CVE-2022-3445, CVE-2022-3448, CVE-2022-3449, CVE-2022-3450 a CVE-2022-3654 umožňujú použiť dealokované miesto v pamäti v komponentoch Skia, Permissions API, Safe Browsing, Peer Connection a Layout.

CVE-2022-3446 a CVE-2022-3653 sú chyby pretečenia medzipamäte haldy v komponentoch WebSQL a Vulkan.

CVE-2022-3447 súvisí s nevhodnou implementáciou v komponente Custom Tabs.

CVE-2022-3652 a CVE-2022-3723 sú chyby súvisiace s neoverením typu premennej v komponente V8.

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/2022/10/
https://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_11.html
https://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_25.html
https://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_27.html

4. Adobe Acrobat a Reader

V produkte Adobe Acrobat a Reader boli v mesiaci október opravené 2 kritické a 4 vysoko závažné zraniteľnosti.

Kritické zraniteľnosti CVE-2022-38450 a CVE-2022-42339 umožňujú útočníkom vykonávať ľubovoľný kód kvôli chybám vedúcim k pretečeniu medzipamäte zásobníka.

Vysoko závažné zraniteľnosti CVE-2022-38437, CVE-2022-38449 a CVE-2022-42342 môžu viesť k úniku obsahu pamäte kvôli chybám zápisu na dealokované miesto v pamäti a čítania mimo povolený rozsah v pamäti. Zraniteľnosť CVE-2022-35691 vedie k odmietnutiu služby aplikácie kvôli dereferencii nulového ukazovateľa.

Zraniteľné systémy:

Acrobat DC 22.002.20212 a staršie
Acrobat Reader DC 22.002.20212 a staršie
Acrobat 2020 20.005.30381 a staršie
Acrobat Reader 2020 20.005.30381 a staršie

Odporúčania:

Odporúčame aktualizáciu na verziu:
Acrobat DC 22.003.20258
Acrobat Reader DC 22.003.20258
Acrobat 2020 20.005.30407
Acrobat Reader 2020 20.005.30407

Zdroje:

https://helpx.adobe.com/security/security-bulletin.html
https://helpx.adobe.com/security/products/acrobat/apsb22-46.html

5. Frameworky

Microsoft .NET Framework

V mesiaci október spoločnosť Microsoft neopravila vo frameworku .NET žiadne kritické, ani vysoko závažné zraniteľnosti.

Zdroje:

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

Oracle Java

V mesiaci október spoločnosť Oracle opravila v platforme Java SE 1 kritickú a 1 vysoko závažnú zraniteľnosť.

Kritická zraniteľnosť CVE-2022-32215 sa nachádza v komponente Node.js a umožňuje útočníkom prenášať škodlivé http požiadavky. Vysoko závažná zraniteľnosť CVE-2022-21634 umožňuje neautentifikovanému útočníkovi kompromitovať zraniteľnú verziu platformy a spôsobiť odmietnutie služby.

Zraniteľné systémy:

Oracle GraalVM Enterprise Edition 20.3.7, 21.3.3 a 22.2

Odporúčania:

Odporúčame aktualizáciu Oracle GraalVM Enterprise Edition na najnovšiu verziu.

Zdroje:

https://www.oracle.com/technetwork/topics/security/alerts-086861.html
https://www.oracle.com/security-alerts/cpuoct2022.html#AppendixJAVA
https://nvd.nist.gov/vuln/detail/CVE-2022-32215
https://nvd.nist.gov/vuln/detail/CVE-2022-21634

6. Iné závažné zraniteľnosti

Zero-day zraniteľnosti servera Microsoft Exchange

V produkte Microsoft Exchange a jeho súčasti Outlook Web App (OWA) boli objavené dve zraniteľnosti, pre ktoré aktuálne nie je dostupná bezpečnostná oprava, no existuje spôsob dočasnej opravy. Potenciálny vzdialený a autentifikovaný útočník by mohol zneužitím zraniteľností prevziať kontrolu nad serverom a nasadiť škodlivý webshell. Viac informácií na stránke.

Závažné zraniteľnosti vo firmvéri BIOS na zariadeniach Lenovo

Spoločnosť Lenovo opravila novou aktualizáciou 5 zraniteľností vo firmvéri BIOS pre svoje produkty. Tieto zraniteľnosti predstavovali bezpečnostné riziká pre stovky zariadení Lenovo. Išlo najmä o možný únik dát, eskaláciu privilégií, nedostupnosť služieb či vzdialené vykonávanie kódu. Viac informácií na stránke.

Kritická zraniteľnosť Fortinet

V produkte FortiOS a FortiProxy sa nachádza zraniteľnosť, ktorá môže umožniť vzdialenému a neoverenému útočnikovi obísť autentifikáciu administračného webového rozhrania. Viac informácií na stránke.