Mesačný prehľad kritických zraniteľností máj 2022

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci máj 6 kritických a 58 vysoko závažných zraniteľností súvisiacich s operačným systémom Windows.

Opravené boli kritické zraniteľnosti CVE-2022-21972 a CVE-2022-23270 v protokole point-to-point (PPP), umožňujúce vzdialené vykonávanie kódu.

Ďalšou odstránenou v májovom balíku opráv bola zraniteľnosť CVE-2022-22017 v nástroji Remote Desktop Client. Tiež umožňovala vzdialené vykonávanie kódu.

Poslednou opravenou kritickou zraniteľnosťou umožňujúcou vzdialené vykonávanie kódu bola CVE-2022-26937. Nachádza sa v protokole Windows Network File System (NFS).

Kritické zraniteľnosti CVE-2022-26923 v Active Directory Domain Services a CVE-2022-26931 v autentifikačnom protokole Kerberos umožňovali eskaláciu privilégií.

Zraniteľné systémy:

Windows Server 2012 R2 (Server Core installation)
Windows Server 2012 R2
Windows Server 2012 (Server Core installation)
Windows Server 2012
Windows RT 8.1
Windows 8.1 for x64-based systems
Windows 8.1 for 32-bit systems
Windows Server 2016 (Server Core installation)
Windows Server 2016
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1607 for 32-bit Systems
Windows 10 for x64-based Systems
Windows 10 for 32-bit Systems
Windows 10 Version 21H2 for x64-based Systems
Windows 10 Version 21H2 for ARM64-based Systems
Windows 10 Version 21H2 for 32-bit Systems
Windows 11 for ARM64-based Systems
Windows 11 for x64-based Systems
Windows Server, version 20H2 (Server Core Installation)
Windows 10 Version 20H2 for ARM64-based Systems
Windows 10 Version 20H2 for 32-bit Systems
Windows 10 Version 20H2 for x64-based Systems
Windows Server 2022 Azure Edition Core Hotpatch
Windows Server 2022 (Server Core installation)

Windows Server 2022
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 Server 2019 (Server Core installation)
Windows Server 2019
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1909 for ARM64-based Systems
Windows 10 Version 1909 for x64-based Systems
Windows 10 Version 1909 for 32-bit Systems
Remote Desktop client for Windows Desktop

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-2022-21972
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22017
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23270
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26923
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26931
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26937

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft opravila v mesiaci máj 4 závažné zraniteľnosti. Zraniteľnosť CVE-2022-29107 umožňuje obchádzať bezpečnostné prvky. Ďalšie tri zraniteľnosti umožňujú vzdialené vykonávanie kódu. CVE-2022-29108 sa nachádza v produkte Microsoft SharePoint Server, CVE-2022-29109 a CVE-2022-29110 v Microsoft Excel.

Zraniteľné systémy:

Microsoft Office Web Apps Server 2013 Service Pack 1
Microsoft Excel 2013 Service Pack 1 (64-bit editions)
Microsoft Excel 2013 Service Pack 1 (32-bit editions)
Microsoft Excel 2013 RT Service Pack 1
Microsoft Word 2013 Service Pack 1 (64-bit editions)
Microsoft Word 2013 Service Pack 1 (32-bit editions)
Microsoft Word 2013 RT Service Pack 1

Microsoft Publisher 2013 Service Pack 1 (64-bit editions)
Microsoft Publisher 2013 Service Pack 1 (32-bit editions)
Microsoft Excel 2016 (64-bit edition)
Microsoft Excel 2016 (32-bit edition)
Microsoft Office LTSC 2021 for 32-bit editions
Microsoft Office LTSC 2021 for 64-bit editions
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft Office Online Server
Microsoft Office 2019 for 64-bit editions
Microsoft Office 2019 for 32-bit editions
Microsoft Publisher 2016 (64-bit edition)
Microsoft Publisher 2016 (32-bit edition)
Microsoft Word 2016 (64-bit edition)
Microsoft Word 2016 (32-bit edition)
Microsoft SharePoint Foundation 2013 Service Pack 1
Microsoft SharePoint Server Subscription Edition
Microsoft SharePoint Server 2019
Microsoft SharePoint Enterprise Server 2016

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-2022-29107
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29108
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29109
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29110

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft neopravila tento mesiac v prehliadači Internet Explorer žiadnu kritickú ani závažnú zraniteľnosť.

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

Microsoft Edge

Spoločnosť Microsoft neopravila tento mesiac v prehliadači Edge žiadnu kritickú ani závažnú zraniteľnosť.

Zdroje:

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

Mozilla Firefox

V mesiaci máj boli v prehliadači Firefox a Firefox ESR opravené 2 kritické a 14 závažných zraniteľností.

Kritická zraniteľnosť CVE-2022-1802 umožňuje manipuláciu s JavaScript prototypmi v implementácii top level await. Ak útočník dokáže manipulovať s metódami JavaScript objektu Array, dokáže získať možnosť vykonávať vlastný kód JavaScript s vyššími oprávneniami.

Druhá opravená kritická zraniteľnosť s označením CVE-2022-1529 umožňuje manipuláciu s JavaScript prototypmi tým, že pri indexácii JavaScript objektov sa môže použiť nedôveryhodný vstup. Útočník tak môže získať schopnosť vykonávať JavaScript kód v rodičovskom procese.

Závažná zraniteľnosť CVE-2022-29909 umožňuje obísť výzvu pre potvrdenie povolenia vo vnorenom kontexte prehliadania. CVE-2022-29911 umožňuje obchádzať sandboxovanie objektov iframe. CVE-2022-29914 umožňuje obchádzať notifikácie v režime celej obrazovky. CVE-2022-29916 môže viesť k úniku informácií o histórii prehliadania zneužitím premenných CSS. CVE-2022-29917 a CVE-2022-29918 združujú nešpecifikované bezpečnostné chyby pamäte, ktoré by mohli viesť k vykonávaniu kódu.

Závažná zraniteľnosť CVE-2022-31736 môže viesť k úniku informácií o dĺžke Cross-origin resource. CVE-2022-31737 súvisí s pretečením medzipamäte haldy vo WebGL. CVE-2022-31738 dovoľuje falšovať okná prehliadača v režime celej obrazovky. CVE-2022-31739 umožňuje útočníkovi ovplyvňovať cestu ukladania sťahovaných súborov v OS Windows. CVE-2022-31740 spôsobuje problém pri alokácii registrov pre kód WASM na procesoroch arm64. CVE-2022-31741 súvisí s neinicializovanou premennou, čo môže viesť k čítaniu neplatnej časti pamäte a k poškodeniu pamäte. CVE-2022-31747 a CVE-2022-31748 združujú nešpecifikované bezpečnostné chyby pamäte, ktoré by mohli viesť k vykonávaniu kódu.

Zraniteľné systémy:

Mozilla Firefox verzie staršej ako 101

Mozilla Firefox ESR verzie staršej ako 91.10

Odporúčania:
Odporúčame aktualizáciu Firefox na verziu 101 a Firefox ESR na verziu 91.10.

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-16/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-19/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-20/

Google Chrome
V mesiaci máj bola vydaná oprava 1 kritickej a 21 závažných zraniteľností. Kritická zraniteľnosť CVE-2022-1853 súvisí s možnosťou použitia odalokovaného miesta v pamäti v databáze IndexedDB.

Závažné zraniteľnosti sa väčšinou týkajú pretečenia medzipamäte haldy, čítania mimo povolených hodnôt, nesprávnej implementácie a použitia odalokovaného miesta v pamäti. Zraniteľnosti sa nachádzajú v komponentoch Windows Manager, Performance Manager, Performance APIs, Permission Prompts, Messaging, DevTools, UI Foundations, Sharing, ANGLE, V8 a ďalších.

Zraniteľné systémy:
Google Chrome pre Windows, Mac a Linux verzie staršej ako 102.0.5005.61.

Odporúčania:
Odporúčame aktualizáciu prehliadača Chrome pre Windows, Mac a Linux na verziu 102.0.5005.61.

Zdroje:
https://chromereleases.googleblog.com/2022
https://chromereleases.googleblog.com/2022/05/stable-channel-update-for-chromeos.html
https://chromereleases.googleblog.com/2022/05/stable-channel-update-for-desktop_10.html
https://chromereleases.googleblog.com/2022/05/long-term-support-channel-update.html
https://chromereleases.googleblog.com/2022/05/stable-channel-update-for-desktop_24.html
https://chromereleases.googleblog.com/2022/05/long-term-support-channel-update-for.html

4. Adobe Acrobat a Reader
V produkte Adobe Acrobat a Reader neboli v mesiaci máj opravené žiadne kritické ani závažné zraniteľnosti.

Zdroje:
https://helpx.adobe.com/security.html

5. Frameworky

Microsoft .NET Framework

V mesiaci máj spoločnosť Microsoft opravila 3 závažné zraniteľnosti vo frameworku .NET. Všetky tri zraniteľnosti s číslami CVE-2022-23267, CVE-2022-29117 a CVE-2022-29145 môžu viesť k vyvolaniu nedostupnosti služby.

Zraniteľné systémy:

.NET 5.0
.NET 6.0
.NET Core 3.1

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-2022-23267
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29117
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29145

Oracle Java

Veľká sada opráv je plánovaná na 19. júla 2022.

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

6. Iné závažné zraniteľnosti

Aktívne zneužívaná kritická zraniteľnosť F5 BIG-IP

Zariadenia BIG-IP obsahujú kritickú zraniteľnosť, ktorá umožňuje neautentifikovaným útočníkom prevziať kontrolu nad zraniteľným systémom, vytvárať a mazať súbory a kontrolovať služby. Pre zraniteľnosť existuje verejne dostupný kód pre jej zneužitie a útočníci ju aktívne zneužívajú. Viac informácií na stránke.

Follina: zero-day, zero-click zraniteľnosť Microsoft Office

Bezpečnostní výskumníci objavili vzorky škodlivých súborov Microsoft Office, ktoré zneužívali zero-day zraniteľnosť umožňujúcu vykonávanie ľubovoľného kódu. Zneužitie zraniteľnosti nevyžaduje povolené makrá a v prípade RTF súborov postačí automatické zobrazenie náhľadu vo Windows Explorer. Aktuálne nebola vydaná opravná aktualizácia a pre to odporúčame urgentne nasadiť mitigáciu. Viac informácií na stránke.