Mesačný prehľad kritických zraniteľností jún 2022

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci jún 3 kritické a 36 vysoko závažných zraniteľností súvisiacich s operačným systémom Windows.

Opravené kritické zraniteľnosti umožňujú vzdialené vykonávanie kódu. Zraniteľnosti CVE-2022-30136 a CVE-2022-30163 sa nachádzajú vo virtualizačnej platforme Hyper-V a CVE-2022-30139 v protokole LDAP.

Zraniteľnosti vysokej závažnosti umožňujú vzdialené vykonávanie kódu, eskaláciu oprávnení, predstieranie cudzej identity a obídenie bezpečnostných prvkov. 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 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
Windows Server, version 20H2 (Server Core Installation)
AV1 Video Extension
HEVC Video Extension
HEVC Video Extensions

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-2022-30136
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30139
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30163

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft opravila v mesiaci jún 8 závažných zraniteľností. Zraniteľnosti CVE-2022-30157, CVE-2022-30158, CVE-2022-30168, CVE-2022-30173 a CVE-2022-30174 umožňujú útočníkom vzdialene vykonávať kód. Zraniteľnosti CVE-2022-30159, CVE-2022-30171 a CVE-2022-30172 môžu viesť k úniku informácií.

Zraniteľné systémy:

Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Excel 2013 RT Service Pack 1
Microsoft Excel 2013 Service Pack 1 (32-bit editions)
Microsoft Excel 2013 Service Pack 1 (64-bit editions)
Microsoft Excel 2016 (32-bit edition)
Microsoft Excel 2016 (64-bit edition)
Microsoft Office LTSC 2021 for 32-bit editions
Microsoft Office LTSC 2021 for 64-bit editions
Microsoft Office Online Server
Microsoft Office Web Apps Server 2013 Service Pack 1
Microsoft Photos
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Microsoft SharePoint Enterprise Server 2016

Microsoft SharePoint Foundation 2013 Service Pack 1
Microsoft SharePoint Server 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

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 jún žiadne opravy kritických a závažných zraniteľností.

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

Microsoft Edge

Spoločnosť Microsoft opravila tento mesiac v prehliadači Edge 2 závažné zraniteľnosti. Zraniteľnosti CVE-2022-33639 a CVE-2022-33680 umožňujú útočníkom eskalovať oprávnenia.

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-2022-33680
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-33639

Mozilla Firefox

V mesiaci jún boli v prehliadači Firefox a Firefox ESR opravené 4 závažné zraniteľnosti.

Závažná zraniteľnosť CVE-2022-34468 v Content-Security-Policy (CSP) sandboxe umožňuje obísť zákaz vykonávania skriptov pre iframe.

Zraniteľnosť CVE-2022-34470 sa nachádza v komponente nsSHistory a súvisí s použitím odalokovaného miesta v pamäti.

CVE-2022-34479 ovplyvňuje iba verziu Firefox pre Linux. Umožňuje zmeniť rozmery vyskakovacieho okna tak, že okno prekryje adresný riadok prehliadača. To umožňuje útočníkom oklamať používateľa a vydávať škodlivú webstránku za legitímnu.

CVE-2022-34484 je sada zraniteľností ovplyvňujúcich bezpečnosť pamäte, ktoré môžu viesť ku poškodeniu pamäte alebo možnosti vykonávať kód.

Zraniteľné systémy:
Mozilla Firefox verzie staršej ako 102
Mozilla Firefox ESR verzie staršej ako 91.11

Odporúčania:
Odporúčame aktualizáciu Firefox na verziu 102 a Firefox ESR na verziu 91.11

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-26/

Google Chrome

V mesiaci jún bola vydaná oprava 1 kritickej a 6 závažných zraniteľností. Kritická zraniteľnosť CVE-2022-2156 sa nachádza v komponente Base a súvisí s možnosťou použitia dealokovaného miesta v pamäti.

Závažné zraniteľnosti CVE-2022-2007 v komponente WebGPU, CVE-2022-2011 v ANGLE a CVE-2022-2157 v Interest groups umožňujú použiť dealokované miesto v pamäti. Závažná zraniteľnosť CVE-2022-2008 v komponente WebGL dovoľuje prístup k pamäti mimo

povolených hodnôt, CVE-2022-2010 umožňuje čítanie pamäte mimo povolených hodnôt a CVE-2022-2158 vo V8 súvisí s neoverovaním typu premennej.

Zraniteľné systémy:
Google Chrome pre Windows, Mac a Linux verzie staršej ako 103.0.5060.53.

Odporúčania:
Odporúčame aktualizáciu prehliadača Chrome pre Windows, Mac a Linux na verziu 103.0.5060.53.

Zdroje:
https://chromereleases.googleblog.com/2022
https://chromereleases.googleblog.com/2022/06/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2022/06/stable-channel-update-for-desktop_21.html

4. Adobe Acrobat a Reader

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

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

5. Frameworky

Microsoft .NET Framework

V mesiaci jún spoločnosť Microsoft opravila 1 závažnú zraniteľnosť vo frameworku .NET. Zraniteľnosť s číslom CVE-2022-30184 môže viesť k úniku informácií.

Zraniteľné systémy:
.NET Core 3.1
.NET 6.0

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

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

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.