Mesačný prehľad kritických zraniteľností apríl 2022

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci apríl 9 kritických a 92 závažných zraniteľností súvisiacich s operačným systémom Windows.

Kritické zraniteľnosti CVE-2022-24541, CVE-2022-26809, CVE-2022-26919, CVE-2022-24537, CVE-2022-24491, CVE-2022-24500, CVE-2022-23259, CVE-2022-23257, CVE-2022-22008, CVE-2022-24497 umožňujú vzdialené vykonanie kódu a vyskytujú sa v systémoch Windows Server Services, Hyper-V, Network File System a v protokoloch LDAP a SMB.

Zraniteľné systémy:

Windows Server Services
Windows Hyper-V
Windows Network File System
Protocol LDAP
Protocol SMB
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1809 for x64-based 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 (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 10 Version 1909 for ARM64-based Systems
Windows 10 Version 1909 for x64-based Systems
Windows 10 Version 1909 for 32-bit Systems
Windows Server 2019 (Server Core installation)
Windows Server 2019
Windows 10 Version 1809 for ARM64-based Systems

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 2012 R2 (Server Core installation)
Windows Server 2012 R2
Windows Server 2012 (Server Core installation)
Windows Server 2012
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 Upgrade Assistant
HEVC Video Extensions
HEVC Video Extension

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://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2022-24541

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2022-26809

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2022-26919

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2022-24537

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2022-24491

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2022-24500

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2022-23257

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2022-22008

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2022-24497

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft opravila v mesiaci apríl 6 závažných zraniteľností. Tri zo závažných zraniteľností (CVE-2022-26903, CVE-2022-26901, CVE-2022-24473) umožňujú útočníkom vzdialené vykonávanie kódu. Zneužitie zraniteľnosti CVE-2022-26911 môže viesť ku odhaleniu informácií. Dve zo závažných zraniteľností (CVE-2022-26910, CVE-2022-24472) umožňujú útočníkom falšovanie a zneužitie legitímnej identity.

Zraniteľné systémy:

Microsoft Lync Server 2013 CU10
Skype for Business Server 2019 CU6
Skype for Business Server 2015 CU12
Microsoft SharePoint Foundation 2013 Service Pack 1
Microsoft SharePoint Server 2016
Microsoft SharePoint Server Subscription Edition
Microsoft SharePoint Server 2019
Microsoft SharePoint Enterprise Server 2016
Microsoft PowerPoint Mobile
Microsoft Excel Mobile
Microsoft Word Mobile
Microsoft PowerPoint for Android
Microsoft Excel for Android
Microsoft Office Web Apps Server 2013 Service Pack 1
Microsoft Office 2013 Service Pack 1 (64-bit editions)
Microsoft Office 2013 Service Pack 1 (32-bit editions)
Microsoft Office 2013 RT 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 Office 2016 (64-bit edition)
Microsoft Office 2016 (32-bit edition)
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 Office LTSC for Mac 2021
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 Mac

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 Edge

Spoločnosť Microsoft opravila tento mesiac v prehliadači Edge 7 závažných zraniteľností.

Zneužitie týchto zraniteľností (CVE-2022-29144, CVE-2022-26908, CVE-2022-26900, CVE-2022-26895, CVE-2022-26894, CVE-2022-26891, CVE-2022-24475) môže viesť ku eskalácii privilégií útočníkom, čo by mohlo mať za následok únik informácií.

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

Mozilla Firefox

V mesiaci apríl boli v prehliadači Mozilla Firefox opravené 3 závažné zraniteľnosti.

CVE-2022-1097 - objekty NSSToken boli odkazované cez priame body a mohlo sa k nim pristupovať nezabezpečenými spôsobmi. To by mohlo viesť k použitiu odalokovaného miesta v pamäti.

CVE-2022-28281 - Ak by kompromitovaný proces odoslal neočakávaný počet WebAuthN rozšírení v príkaze Register nadradenému procesu, došlo by ku zápisu mimo povolených hodnôt, čo by viedlo ku poškodeniu pamäte a potenciálne zneužiteľnému zlyhaniu.
CVE-2022-28289 - Vývojári Mozilla nahlásili chyby bezpečnosti pamäte prítomné vo Firefox 98 a Firefox ESR 91.7. Niektoré z nich by mohli byť pri dostatočnom úsilí zneužité na vykonanie ľubovoľného kódu.

Zraniteľné systémy:

Mozilla Firefox verzie staršej ako 98
Mozilla Firefox ESR verzie staršej ako 91.7

Odporúčania:

Odporúčame aktualizáciu Firefox na verziu 98 a Firefox ESR na verziu 91.7.

Zdroje:

https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-14/#CVE-2022-1097
https://www.mozilla.org/en-US/security/advisories/mfsa2022-14/#CVE-2022-28281
https://www.mozilla.org/en-US/security/advisories/mfsa2022-14/#CVE-2022-28289

Google Chrome

V mesiaci apríl bola vydaná oprava na 14 závažných zraniteľností.

Deväť závažných zraniteľností umožňuje použitie odalokovaného miesta v pamäti. Ich zneužitie by mohlo viesť k vykonaniu ľubovoľného kódu.

CVE-2022-1364 - Zraniteľnosť súvisí s nesprávnou optimalizáciou JIT kompilácie

CVE-2022-1482 - nevhodná implementácia v softvérovej knižnici WebGL

CVE-2022-1483 - Pretečenie vyrovnávacej pamäte haldy vo WebGPU

CVE-2022-1096 - Vedľajší účinok v zachytávači CSSStyleDeclaration vedie k poškodeniu objektu JS

CVE-2022-1364 - Nekompletná oprava pre CVE-2022-1096. Neoverenie typu premennej vo V8.

Zraniteľné systémy:
Google Chrome pre Windows, Mac a Linux verzie staršej ako 96.0.4664.207 s dlhodobou podporou a 100.0.4896.143 s rozšíreným stabilným kanálom.

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

Zdroje:
Chrome Releases: 2022 (googleblog.com)
Chrome Releases: April 2022 (googleblog.com)

4. Acrobat a Reader

V produkte Adobe Acrobat a Reader bolo v mesiaci apríl opravených 35 kritických a 24 závažných zraniteľnosti.

22 kritických zraniteľností (CVE-2022-24103, CVE-2022-24104, CVE-2022-27785, CVE-2022-24102, CVE-2022-27786, CVE-2022-27789, CVE-2022-27790, CVE-2022-27795, CVE-2022-27796, CVE-2022-27797, CVE-2022-27799, CVE-2022-27800, CVE-2022-27801, CVE-2022-27802, CVE-2022-28230, CVE-2022-28232, CVE-2022-28233, CVE-2022-28235, CVE-2022-28237, CVE-2022-28238, CVE-2022-28240, CVE-2022-28242) umožňuje použitie odalokovaného miesta na pamäti. Ich zneužitie by mohlo viesť ku vykonaniu ľubovoľného kódu.

10 kritických zraniteľností (CVE-2022-27787, CVE-2022-27788, CVE-2022-27792, CVE-2022-27793, CVE-2022-27798, CVE-2022-28231, CVE-2022-28236, CVE-2022-28239, CVE-2022-28241, CVE-2022-28243) umožňuje zápis mimo povolených hodnôt čo by mohlo mať za následok vykonanie ľubovoľného kódu.

Zneužitie kritických zraniteľnosti (CVE-2022-24102, CVE-2022-27788) umožňuje vykonanie ľubovoľného kódu.

Zneužitie závažnej zraniteľnosti CVE-2022-27788 môže mať za následok únik pamäte.

Zraniteľné systémy:
Acrobat DC 22.001.20085 and earlier versions

Acrobat Reader DC 22.001.20085 and earlier versions

Acrobat 2020 20.005.30314 and earlier versions (Windows) 20.005.30311 and earlier versions (macOS)

Acrobat Reader 2020 20.005.30314 and earlier versions (Windows) 20.005.30311 and earlier versions (macOS)

Acrobat 2017 17.012.30205 and earlier versions

Acrobat Reader 2017 17.012.30205 and earlier versions

Zdroje:
https://helpx.adobe.com/security.html
Adobe Security Bulletin

5. Frameworky

Microsoft .NET Framework

V mesiaci apríl bola opravená 1 závažná zraniteľnosť.

Zneužitie zraniteľnosti CVE-2022-26832 môže vyvolať nedostupnosť služieb.

Zraniteľné systémy:

Microsoft .NET Framework 3.5 a 4.7.2
Microsoft .NET Framework 3.5 a 4.8
Microsoft .NET Framework 4.8
Microsoft .NET Framework 4.5.2
Microsoft .NET Framework 3.5.1
Microsoft .NET Framework 3.5
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2
Microsoft .NET Framework 2.0 Service Pack 2
Microsoft .NET Framework 3.0 Service Pack 2
Microsoft .NET Framework 4.6

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-2022-26832

Oracle Java

Spoločnosť Oracle opravila v mesiaci apríl 3 závažné zraniteľnosti.

Zneužitie zraniteľnosti CVE-2022-0778 môže spôsobiť nedostupnosť služieb.
Zneužitie zraniteľností CVE-2022-21449, CVE-2022-21476 umožňuje neautorizovanému a neautentifikovanému útočníkovi získať prístup ku citlivým dátam.

Zraniteľné systémy:

Oracle GraalVM Enterprise Edition: 20.3.5, 21.3.1, 22.0.0.2
Oracle Java SE: 17.0.2, 18; Oracle GraalVM Enterprise Edition: 21.3.1, 22.0.0.2
Oracle Java SE: 7u331, 8u321, 11.0.14, 17.0.2, 18; Oracle GraalVM Enterprise Edition: 20.3.5, 21.3.1, 22.0.0.2

Odporúčania:

Odporúčame aktualizovať zraniteľné verzie Java SE a Java SE Embedded na aktuálne verzie, prostredníctvom Java Auto Update alebo na stránke spoločnosti Oracle, viď prvý odkaz v zdrojoch.

Zdroje:

Oracle Critical Patch Update Advisory - April 2022
Text Form of Oracle Critical Patch Update - April 2022 Risk Matrices

6. Iné závažné zraniteľnosti

Masívna phishingová kampaň zneužíva ukradnutú e-mailovú komunikáciu

Aktuálna phishingová kampaň šíri malvér v odpovedi na legitímnu komunikáciu. Týmto spôsobom sa snaží zmiasť obeť a presvedčiť ju, že otvára dokument od dôveryhodnej osoby. Apelujeme na zvýšenú obozretnosť pri prijímaní e-mailových správ s priloženými súbormi, či webovými odkazmi v tele. Viac informácií na stránke.

Spring4Shell – kritická zraniteľnosť open source Java frameworku Spring

Spring Framework obsahuje ľahko zneužiteľnú kritickú zraniteľnosť, ktorá umožňuje neautentifikovanému útočníkovi vzdialene vykonávať kód. Spoločnosť VMware, ktorá framework vyvíja, odporúča čo najskôr aktualizovať zraniteľné aplikácie, alebo ak to nie je možné, využiť dočasné možnosti zabránenia zneužitiu zraniteľnosti. Postup zneužitia je verejne dostupný. Viac informácií na stránke.

Zraniteľnosť služby Gitlab

Dňa 31.3.2022 spoločnosť Gitlab objavila kritickú zraniteľnosť v ich službe, ktorá má CVSSv3 skóre 9.1. Zraniteľnosť spočíva v ukladaní prednastaveného hesla v zdrojovom kóde. Viac informácií na stránke.

SonicWall – kritická zraniteľnosť v SonicOS

Spoločnosť SonicWall vydala bezpečnostné aktualizácie pre viacero firewallov, ktoré by mohli byť zneužité neautentifikovanými útočníkmi pre vzdialené vykonávanie kódu. Zraniteľnosť je kritickej závažnosti s CVSSv3 skóre 9.4. Viac informácií na stránke.

Závažná zraniteľnosť OpenSSL umožňuje DoS

V knižnici OpenSSL sa nachádza zraniteľnosť, pomocou ktorej môže útočník zahltiť systém tak, že vytvorí nekonečnú slučku v napadnutej službe. Jedná sa o zraniteľnosť vysokej závažnosti s CVSSv3 skóre 7.5. Viac informácií na stránke.

Zero-day zraniteľnosť služby Nginx

V službe Nginx bola objavená zero-day zraniteľnosť, ktorá sa nachádza v module LDAP-auth. Útočník môže po jej zneužití vykonávať kód na diaľku. Spoločnosť Nginx, ktorá službu vyvíja, oznámila, že služby Nginx Open Source a Nginx Plus nie sú zraniteľné. Zraniteľná je iba verzia, ktorá používa implementáciu Nginx reference. Zraniteľnosť je aktívne zneužívaná. Viac informácií na stránke.