Mesačný prehľad kritických zraniteľností
január 2022

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci január 7 kritických a 80 závažných zraniteľností.

Kritická zero-day zraniteľnosť **CVE-2021-22947** sa vyskytuje v knižnici cURL a môže viesť k Man-in-the-Middle útokom. Táto zraniteľnosť spôsobuje, že útočník je schopný injektovať falošné odpovede, následne preniesť TLS z legitímneho servera a oklamať tak nástroj curl, aby zaslal údaje späť používateľovi. Nástroj pritom predpokladá, že údaje injektované útočníkom pochádzajú zo servera chráneného TLS.

Ďalšia zraniteľnosť **CVE-2022-21833** sa nachádza vo Virtual Machine IDE Drive a súvisí s eskaláciou privilégií. Úspešné zneužitie chyby vyžaduje autentifikáciu.

Zraniteľnosť **CVE-2022-21857** sa vyskytuje v Active Directory Domain Services. Útočník je schopný zraniteľnosť zneužiť vzdialene a zvýšiť svoje oprávnenia na zraniteľných systémoch.

Dve kritické zraniteľnosti **CVE-2022-21898** a **CVE-2022-21912** v jadre DirectX Graphics umožňujú vzdialené vykonanie kódu.

Kritická zraniteľnosť **CVE-2022-21907**, označená ako „wormable“ sa nachádza v HTTP Protocol Stack (http.sys). Zneužitím môže dôjsť k vzdialenému vykonaniu kódu. Vzdialený neoverený útočník by mohol poslať špeciálne vytvorený paket na server využívajúci http.sys. Na spustenie a šírenie infekcie nie je potrebná žiadna interakcia používateľa.

Medzi zraniteľnosti umožňujúce RCE tiež patrí **CVE-2022-21917**, ktorá sa vyskytuje v HEVC Video Extensions.

Zraniteľné systémy:

HEVC Video Extensions
Remote Desktop client for Windows Desktop
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 1909 for 32-bit Systems
Windows 10 Version 1909 for ARM64-based Systems
Windows 10 Version 1909 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, version 20H2 (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://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-22947
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2022-21833
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2022-21857
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2022-21898
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2022-21907
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2022-21912
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2022-21917

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft opravila v mesiaci január 1 kritickú a 3 závažné zraniteľnosti. Kritická zraniteľnosť CVE-2022-21840 môže viesť k vzdialenému vykonaniu kódu. Všetky závažné zraniteľnosti (CVE-2022-21837, CVE-2022-21841 a CVE-2022-21842) umožňujú útočníkom vzdialené vykonávanie kódu.

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 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 Office Online Server
Microsoft Office Web Apps Server 2013 Service Pack 1
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 Word 2016 (32-bit edition)
Microsoft Word 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
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2022-21840

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 opravila tento mesiac v prehliadači Edge 4 závažné zraniteľnosti, pričom 2 z nich môžu viesť k vzdialenému vykonaniu kódu a 2 k eskalácii privilégií.

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 január nebola v prehliadači Firefox a Firefox ESR opravená žiadna kritická zraniteľnosť. V prehliadačoch Firefox a Firefox ESR bolo opravených 9 závažných zraniteľností.

CVE-2022-22746 ovplyvňuje prehliadač pre Windows a týka sa súbehu pri volaní funkcie reportValidity. Chyba umožňuje skryť notifikáciu pre stránky, čo dovoľuje útoky typu spoofing. CVE-2022-22743 súvisí s požadovaním prístupu na celú obrazovku. Karta kontrolovaná útočníkom môže spôsobiť, že prehliadač nebude môcť opustiť režim celej

obrazovky. CVE-2022-22741 je tiež zraniteľnosť súvisiaca s režimom celej obrazovky. Pri zmene veľkosti kontextového okna počas žiadosti o prístup na celú obrazovku by kontextové okno nebolo schopné opustiť režim celej obrazovky.

CVE-2022-22742 súvisí s prístupom k pamäti mimo povolených hodnôt pri vkladaní textu v režime úprav. CVE-2022-22740 súvisí s použitím odalokovaného miesta v pamäti. CVE-2022-22738 sa týka pretečenia medzipamäte haldy. CVE-2022-22737 súvisí s konštrukciou zvukových kanálov. Chyba môže viesť k súbehu pri prehrávaní zvukových súborov a zatváraní okien. CVE-2022-4140 umožňuje vytvoriť špecifické značky XSLT, ktoré sú schopné obísť sandbox.

CVE-2021-22751 vyskytujúca sa v prehliadačoch Firefox 95 a v Firefox ESR 91.4 je séria chýb zabezpečenia v pamäti, z ktorých niektoré majú potenciál zneužitia pre vykonávanie ľubovoľného kódu.

Zraniteľné systémy:
Mozilla Firefox verzie staršej ako 96
Mozilla Firefox ESR verzie staršej ako 91.5

Odporúčania:
Odporúčame aktualizáciu Firefox na verziu 96 a Firefox ESR na verziu 91.5.

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-01/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-02/

Google Chrome

V mesiaci január bola vydaná oprava pre 2 kritické a 25 závažných zraniteľností.

Kritická zraniteľnosť CVE-2022-0096 súvisí s použitím odalokovaného miesta v pamäti v komponente Storage. Druhá kritická zraniteľnosť CVE-2022-0289 sa týka tiež použitia odalokovaného miesta v pamäti v komponente Safe browsing.

Závažné zraniteľnosti sa týkajú nesprávnej implementácie, pretečenia medzipamäte haldy a použitia odalokovaného miesta v pamäti. Zraniteľnosti sa nachádzajú v komponentoch DevTools, V8, Bookmarks, Autofill a ďalších.

Zraniteľné systémy:
Google Chrome verzie staršej ako 97.0.4692.99

Odporúčania:
Odporúčame aktualizáciu na verziu 97.0.4692.99

Zdroje:
https://chromereleases.googleblog.com/2022
https://chromereleases.googleblog.com/2022/01/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2022/01/stable-channel-update-for-desktop_19.html

4. Adobe Acrobat a Reader

V produkte Adobe Acrobat a Reader bolo opravených 15 kritických zraniteľností. Šesť z týchto zraniteľností (CVE-2021-44701, CVE-2021-44704, CVE-2021-44706, CVE-2021-44710, CVE-2021-45062, CVE-2021-45064) súvisí s použitím odalokovaného miesta v pamäti. Zraniteľnosti CVE-2021-45061, CVE-2021-45068 a CVE-2021-44707 sa týkajú zápisu mimo povolených hodnôt, CVE-2021-45060 súvisí s čítaním mimo povolených hodnôt. CVE-2021-44703 súvisí s pretečením medzipamäte zásobníka a zraniteľnosti CVE-2021-44708 a CVE-2021-44709 súvisia s pretečením medzipamäte haldy. CVE-2021-44705 sa týka prístupu neinicializovaného ukazovateľa. CVE-2021-44711 súvisí s pretečením premennej typu integer. Zneužitím všetkých týchto zraniteľností sú útočníci schopní vzdialene vykonávať ľubovoľný kód.

Zraniteľné systémy:
Acrobat DC
Acrobat Reader DC
Acrobat 2020
Acrobat Reader 2020
Acrobat 2017
Acrobat Reader 2017

Odporúčania:
Odporúčame aktualizáciu:
Acrobat DC na verziu 21.007.20039
Acrobat Reader DC na verziu 21.007.20039
Acrobat 2020 na verziu 20.004.30020
Acrobat Reader 2020 na verziu 20.004.30020
Acrobat 2017 na verziu 17.011.30207
Acrobat Reader 2017 na verziu 17.011.30207

Zdroje:
https://helpx.adobe.com/security.html
https://helpx.adobe.com/security/products/acrobat/apsb22-01.html

5. Frameworky

Microsoft .NET Framework

V mesiaci január spoločnosť Microsoft opravila 1 závažnú zraniteľnosť vo frameworku .NET. Zneužitím zraniteľnosti CVE-2022-21911 môže dôjsť k narušeniu dostupnosti služby.

Zraniteľné systémy:
Microsoft .NET Framework 2.0 Service Pack 2
Microsoft .NET Framework 3.5, 3.5.1
Microsoft .NET Framework 4.5.2
Microsoft .NET Framework 4.6, 4.6.1, 4.6.2
Microsoft .NET Framework 4.7, 4.7.1, 4.7.2
Microsoft .NET Framework 4.8

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

Spoločnosť Oracle vydala v mesiaci január plánovanú štvrťročnú veľkú sadu aktualizácií. V Oracle Java SE bolo dokopy opravených 18 zraniteľností, z čoho ani jedna nebola kritická alebo závažná.

Zraniteľné systémy:
Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01
Oracle GraalVM Enterprise Edition: 20.3.4, 21.3.0

Odporúčania:
Odporúčame aktualizovať zraniteľné verzie Oracle GraalVM Enterprise Edition a Java SE na aktuálne verzie, prostredníctvom Java Auto Update alebo na stránke spoločnosti Oracle, viď

prvý odkaz v zdrojoch.

Zdroje:
https://www.oracle.com/security-alerts/
https://www.oracle.com/security-alerts/cpujan2022.html

6. Iné závažné zraniteľnosti

Spoločnosť Microsoft opravila 97 zraniteľností, z toho 9 kritických a 6 zero-day

Spoločnosť Microsoft vydala balík opráv Patch Tuesday, v ktorom opravila 97 zraniteľností. Deväť z nich bolo označených ako kritickéh a 88 ako závažné. Až 6 z týchto zraniteľností je typu zero-day. Zneužitím týchto zraniteľností môže dôjsť napríklad k vzdialenému vykonaniu kódu, eskalácii privilégií alebo narušeniu dostupnosti služby. Avšak jedna z najnovších aktualizácií pre Windows Server (KB5009624, KB5009557 a KB5009555, KB5009566 a KB5009543) spôsobuje problémy s doménovými radičmi. Preto je potrebné zvážiť jej nasadenie. Viac informácií na stránke.

PwnKit – závažná zraniteľnosť vyskytujúca sa v predvolených inštaláciách rôznych distribúcií Linuxu

Závažná zraniteľnosť PwnKit (CVE-2021-4034), ktorá sa môže vyskytovať vo všetkých distribúciách Linuxu, môže viesť k eskalácii privilégií až na oprávnenia root. Nachádza sa v programe pkexec komponentu PolicyKit, ktorý je možné použiť na vykonávanie príkazov s právami používateľa root. Viac informácií na stránke.