Mesačný prehľad kritických zraniteľností december 2023

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci december 3 kritické a 22 vysoko závažných zraniteľností.

Kritická zraniteľnosť CVE-2023-35628 sa nachádza v komponente Windows MSHTML. Útočník môže túto zraniteľnosť zneužiť odoslaním špeciálne vytvoreného mailu, ktorého obsah sa automaticky spustí pri načítaní a spracovaní mailovým klientom. Zneužitie zraniteľnosti by mohlo útočníkovi umožniť vzdialené vykonávanie kódu.

Zraniteľnosti CVE-2023-35630 a CVE-2023-35641 sa týkajú služby Internet Connection Sharing (ICS) a umožňujú vzdialené vykonávanie kódu. Úspešné zneužitie CVE-2023-35630 vyžaduje, aby útočník zmenil pole option->length vo vstupnej správe protokolu DHCPv6, DHCPV6_MESSAGE_INFORMATION_REQUEST. Pre zneužitie zraniteľnosti CVE-2023-35641 musí útočník odoslať škodlivo vytvorenú správu na DHCP server, na ktorom beží služba Internet Connection Sharing (ICS).

Vysoko závažné zraniteľnosti umožňujú eskaláciu oprávnení a narušenie dostupnosti služby. Zneužitie niektorých z nich môže viesť k úniku informácií, vzdialenému vykonávaniu kódu alebo predstieraniu/falšovaniu identity.

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 21H2 for 32-bit Systems
Windows 10 Version 21H2 for ARM64-based Systems
Windows 10 Version 21H2 for x64-based Systems
Windows 10 Version 22H2 for 32-bit Systems
Windows 10 Version 22H2 for ARM64-based Systems
Windows 10 Version 22H2 for x64-based Systems
Windows 11 version 21H2 for ARM64-based Systems
Windows 11 version 21H2 for x64-based Systems
Windows 11 Version 22H2 for ARM64-based Systems
Windows 11 Version 22H2 for x64-based Systems
Windows 11 Version 23H2 for ARM64-based Systems
Windows 11 Version 23H2 for x64-based Systems

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, 23H2 Edition (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://msrc.microsoft.com/update-guide/en-us
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35628
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35630
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35641

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť opravila v mesiaci december 3 vysoko závažné zraniteľnosti.

Vysoko závažné zraniteľnosti CVE-2023-35619 a CVE-2023-35636 sa nachádzajú v aplikácii Microsoft Outlook. Zraniteľnosť CVE-2023-35619 môže útočníkovi dovoliť predstieranie/falšovanie identity na zariadeniach Mac. Pre úspešné zneužitie CVE-2023-35636 musí útočník presvedčiť svoju obeť, aby klikla na podvrhnutý odkaz a otvorila špeciálne vytvorený súbor. Táto chyba umožňuje útočníkom pristupovať k NTLM hašom.

Zraniteľnosť CVE-2023-36009 sa nachádza v aplikácii Microsoft Word a vyžaduje od obete spustenie škodlivého súboru. Úspešné zneužitie umožňuje neautorizovanému útočníkovi pristupovať a čítať v súborovom systéme.

Zraniteľné systémy:

Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
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 LTSC 2021 for 32-bit editions
Microsoft Office LTSC 2021 for 64-bit editions
Microsoft Office LTSC for Mac 2021

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://msrc.microsoft.com/update-guide/en-us
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35619
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35636
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36009

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft ukončila podporu prehliadača Internet Explorer 15.6.2022 pre hlavnú líniu operačných systémov Windows 10 a 11. Pre zvyšné operačné systémy, kde je prehliadač ešte podporovaný, nevydala v mesiaci december žiadne opravy kritických a závažných zraniteľností.

Odporúčania:

Odporúčame prestať používať a odinštalovať Internet Explorer a nahradiť ho podporovaným prehliadačom Microsoft Edge.

Zdroje:

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

Microsoft Edge

Spoločnosť Microsoft v mesiaci december neopravila v prehliadači Microsoft Edge žiadne kritické ani závažné zraniteľnosti.

Zdroje:

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

Mozilla Firefox

V mesiaci december bolo opravených 5 vysoko závažných zraniteľností v línii Firefox a Firefox ESR.

Vysoko závažná zraniteľnosť CVE-2023-6856 súvisí s pretečením medzipamäte na halde v komponente WebGL. Táto chyba umožňuje vzdialené vykonávanie kódu a môže viesť k úniku zo sandboxu prehliadača.

Zraniteľnosť CVE-2023-6135 sa nachádza v produkte Firefox, v knižniciach Network Security Services (NSS). Úspešné zneužitie umožňuje útočníkovi získať súkromný kľúč.

CVE-2023-6864 (Firefox 120, Firefox ESR 115.5) a CVE-2023-6873 (Firefox 120) pokrývajú sadu zraniteľností ovplyvňujúcich bezpečnosť pamäte, ktoré môžu viesť ku poškodeniu pamäte alebo možnosti vykonávať kód.

CVE-2023-6865 sa týka triedy EncryptingOutputStream. Úspešné zneužitie umožňuje útočníkovi zapisovať na disk a môže dôjsť k úniku informácií.

Zraniteľné systémy:

Mozilla Firefox verzie staršie ako 121
Mozilla Firefox ESR verzie staršej ako 115.6

Odporúčania:

Odporúčame aktualizáciu Mozilla Firefox na verziu 121 a Mozilla Firefox ESR na verziu 115.6.

Zdroje:

https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-54/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-56/

Google Chrome

V mesiaci december bola vydaná oprava 8 vysoko závažných zraniteľností prehliadača Google Chrome.

Závažná zraniteľnosť CVE-2023-6702 sa nachádza v komponente V8 a súvisí s neoverením typu premennej.

Zraniteľnosti CVE-2023-6703, CVE-2023-6704, CVE-2023-6705, CVE-2023-6706, CVE-2023-6508 a CVE-2023-6509 dovoľujú použiť dealokované miesto v pamäti v komponentoch Blink, libavif, WebRTC, FedCM, Media Stream a Side Panel Search.

Aktívne zneužívaná zraniteľnosť CVE-2023-7024 súvisí s pretečením medzipamäte na halde v komponente WebRTC.

Zraniteľné systémy:

Google Chrome pre Windows verzie staršej ako 120.0.6099.129/.130 a Linux a Mac verzie staršej ako 120.0.6099.129.

Odporúčania:

Odporúčame aktualizáciu prehliadača Chrome pre Windows aspoň na verziu 120.0.6099.129/.130 a Linux a Mac aspoň na verziu 120.0.6099.129.

Zdroje:

https://chromereleases.googleblog.com/
https://chromereleases.googleblog.com/2023/12/stable-channel-update-for-desktop_20.html
https://chromereleases.googleblog.com/2023/12/stable-channel-update-for-desktop_12.html
https://chromereleases.googleblog.com/2023/12/stable-channel-update-for-desktop.html

4. Adobe Acrobat a Reader

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

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

5. Frameworky

Microsoft .NET Framework

V mesiaci december spoločnosť Microsoft neopravila žiadne kritické ani závažné zraniteľnosti vo frameworku .NET.

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

Oracle Java

Veľká sada opráv je plánovaná na 16. januára 2024.

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

6. Iné závažné zraniteľnosti

Vysoko závažná zraniteľnosť v procesoroch AMD

Spoločnosť Microsoft v rámci balíka opráv Patch Tuesday vydala opravu pre 34 zraniteľností. Oprava sa týkala aj 1 zero-day zraniteľnosti v procesoroch AMD a jej úspešné zneužitie môže viesť k úniku informácií. **Viac informácií na stránke.**

Kritické zraniteľnosti v produkte SAP Business Technology Platform

Spoločnosť SAP vydala v decembri 2023 balík opráv pre svoje produkty opravujúcich 15 zraniteľností v Business Technology Platform, 4 z nich sú označené ako kritické. Úspešné zneužitie umožňuje neautentifikovanému útočníkovi eskaláciu privilégií. **Viac informácií na stránke.**

Závažná zraniteľnosť platformy WordPress

Bezpečnostný tím spoločnosti Fenrisk objavil závažnú zraniteľnosť, ktorá sa nachádza v jadre frameworku WordPress. Úspešné zneužitie umožňuje získať neoprávnený prístup ku webstránkam na platforme WordPress a vzdialené vykonávanie kódu. **Viac informácií na stránke.**

Aktívne zneužívaná zraniteľnosť v službe ownCloud

Spoločnosť CISA poukázala na aktívne zneužívanú kritickú zraniteľnosť CVE-2023-49103, ktorá umožňuje únik používateľských údajov a licenčných kľúčov. Boli objavené ďalšie dve kritické zraniteľnosti CVE-2023-49104 a CVE-2023-49105, ktoré umožňujú obídenie autentifikácie. Úspešné zneužitie umožňuje útočníkom získať prístup a kontrolu nad ďalšími službami. **Viac informácií na stránke.**

Android má aktívne zneužívanú zero-click zraniteľnosť

Spoločnosť Google vydala v decembri balík opráv 85 zraniteľností vo svojom systéme Android a jeho komponentoch. Z nich sú 4 označené ako kritické. Jedna z nich je aktívne zneužívaná a

umožňuje vykonávanie ľubovoľného kódu. Útočník pre jej zneužitie nepotrebuje žiadne dodatočné oprávnenia, ani interakciu obete. **Viac informácií na stránke.**

Kritické zraniteľnosti v Atlassian

Spoločnosť Atlassian vydala opravu 4 kritických zraniteľností viacerých svojich produktov. Úspešné zneužitie umožňuje útočníkom vykonať vzdialené vykávanie kódu. Je potrebná bezodkladná aktualizácia. **Viac informácií na stránke.**

Dve kritické zraniteľnosti v službe VMware

Spoločnosť VMware opravila dve kritické zraniteľnosti. Zneužitím zraniteľnosti CVE-2023-34060 môže útočník obísť autentifikáciu vo VMware Cloud Director Appliance. Chyba CVE-2023-34048 vo VMware vCenter Server umožňuje zapisovať mimo povolené hodnoty v pamäti. Úspešné zneužitie umožňuje útočníkovi vzdialené vykonávanie kódu. **Viac informácií na stránke.**

Čínska kyberšpionáž v produktoch Atlassian

Spoločnosť Atlassian plánovane zruší podporu pre produkt Confluence Server. Po dátume 15. februára 2024 aktualizácie zabezpečenia, opravy chýb, technickú podporu a ani aktualizácie technického obsahu online pre produkty Server nebude poskytovať. Spoločnosť Microsoft poukázala na aktívne zneužívané zero-day zraniteľností hackerskou skupinou podporovanou čínskou vládou v produktoch Atlassian Confluence Data Center a Server. Úspešné zneužitie umožňuje zvýšiť privilégiá na administrátora, narušiť integritu a získať heslá používateľov. **Viac informácií na stránke.**