Mesačný prehľad kritických zraniteľností
február 2024

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci február 2 kritické a 41 vysoko závažných zraniteľností.

Kritická zraniteľnosť CVE-2024-21357 sa nachádza v protokole Pragmatic General Multicast (PGM) a týka sa vzdialeného vykonávania kódu. Pre úspešné zneužitie je nevyhnutné aby útočník vykonal dodatočné kroky pred samotným zneužitím na prípravu cieľového prostredia.

Zraniteľnosť CVE-2024-20684 sa nachádza vo virtualizačnej platforme Hyper-V a umožňuje vyvolať nedostupnosť služby.

Zraniteľnosti vysokej závažnosti umožňujú vzdialené vykonávanie kódu, obchádzanie bezpečnostných prvkov, predstieranie cudzej identity a eskaláciu oprávnení. 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 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://portal.msrc.microsoft.com/en-us/security-guidance
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20684
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21357

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť opravila v mesiaci február 1 kritickú a 7 vysoko závažných zraniteľností.

Kritická zraniteľnosť CVE-2024-21413 sa nachádza v e-mailovom klientovi Outlook a umožňuje vzdialené vykonávanie kódu. Chyba sa týka nesprávneho parsovania odkazov cez protokol file:// a umožňuje vytvoriť škodlivý odkaz, ktorý obchádza funkciu Protected View Protocol, čo môže viesť k úniku informácií o lokálnych povereniach NTLM a vzdialenému vykonávaniu kódu (RCE). Úspešné zneužitie umožňuje útočníkovi získať vysoké oprávnenia ktoré zahŕňajú funkcie čítania, zápisu a mazania.

Vysoko závažné zraniteľnosti CVE-2024-20673, CVE-2024-21378, CVE-2024-21379 a CVE-2024-21384 umožňujú vzdialené vykonávanie kódu.

Zraniteľnosti CVE-2024-20695 a CVE-2024-21374 sa týkajú obchádzania bezpečnostných prvkov a chyba CVE-2024-21402 môže viesť k eskalácii oprávnení.

Zraniteľné systémy:

Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Excel 2016 (32-bit edition)
Microsoft Excel 2016 (64-bit edition)
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 Outlook 2016 (32-bit edition)
Microsoft Outlook 2016 (64-bit edition)
Microsoft PowerPoint 2016 (32-bit edition)
Microsoft PowerPoint 2016 (64-bit edition)
Microsoft Publisher 2016 (32-bit edition)
Microsoft Publisher 2016 (64-bit edition)
Microsoft Teams for Android
Microsoft Visio 2016 (32-bit edition)
Microsoft Visio 2016 (64-bit edition)
Microsoft Word 2016 (32-bit edition)
Microsoft Word 2016 (64-bit edition)
Skype for Business 2016 (32-bit)
Skype for Business 2016 (64-bit)
Skype for Business Server 2019 CU7

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-2024-21413
https://thehackernews.com/2024/02/critical-exchange-server-flaw-cve-2024.html

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 február 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 február opravila v prehliadači Microsoft Edge 1 vysoko závažnú zraniteľnosť.

Vysoko závažná zraniteľnosť CVE-2024-26192 môže viesť k úniku zo sandboxu prehliadača a môže viesť k úniku citlivých informácií. Pre úspešné zneužitie je potrebná interakcia zo strany obete so špeciálne vytvorenou webstránkou.

Zraniteľné systémy:

Microsoft Edge (Edge-based) build 122.0.2365.52, (Chromium-based) 122.0.6261.57/.58.

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-2024-26192

Mozilla Firefox

V mesiaci február boli opravené 4 vysoko závažné zraniteľnosti v línii Firefox a Firefox ESR.

Vysoko závažné zraniteľnosti CVE-2024-1553 (Firefox 122, Firefox ESR 115.7) a CVE-2024-1557 (Firefox 122) sa týkajú poškodenia pamäte a umožňujú ľubovoľné vykonávanie kódu.

Chyba CVE-2024-1546 umožňuje pristupovať a čítať mimo povolené hodnoty pamäte.

Zraniteľnosť CVE-2024-1547 sa týka možnosti podvrhnutia vyskakovacieho okna na cudzom webe.

Zraniteľné systémy:

Mozilla Firefox verzie staršie ako Firefox 123
Mozilla Firefox ESR verzie staršej ako 115.8

Odporúčania:

Odporúčame aktualizáciu Mozilla Firefox na verziu 123 a Mozilla Firefox ESR na verziu 115.8.

Zdroje:

https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2024-05/
https://www.mozilla.org/en-US/security/advisories/mfsa2024-06/

Google Chrome

V mesiaci február bola vydaná oprava 6 vysoko závažných zraniteľností prehliadača Google Chrome.

Vysoko závažné zraniteľnosti CVE-2024-1938 a CVE-2024-1939 sa týkajú zámeny typu premennej v komponente V8.

Chyba CVE-2024-1669 umožňuje pristupovať mimo povolené hodnoty pamäte v komponente Blink.

Zraniteľnosti CVE-2024-1284 a CVE-2024-1670 umožňujú použiť dealokované miesto v pamäti v komponente Mojo.

CVE-2024-1283 sa týka pretečenia medzipamäte haldy v komponente Skia.

Zraniteľné systémy:

Google Chrome pre Windows verzie staršej ako 122.0.6261.94/.95 a Linux a Mac verzie staršej ako 122.0.6261.94.

Odporúčania:

Odporúčame aktualizáciu prehliadača Chrome pre Windows aspoň na verziu 122.0.6261.94/.95 a Linux a Mac aspoň na verziu 122.0.6261.94.

Zdroje:

https://chromereleases.googleblog.com/2024/02
https://chromereleases.googleblog.com/2024/02/stable-channel-update-for-desktop_27.html
https://chromereleases.googleblog.com/2024/02/stable-channel-update-for-desktop_20.html
https://chromereleases.googleblog.com/2024/02/stable-channel-update-for-desktop.html

4. Adobe Acrobat a Reader

V produkte Adobe Acrobat a Reader bolo v mesiaci február opravených 7 vysoko závažných zraniteľností.
Vysoko závažné zraniteľnosti CVE-2024-20726, CVE-2024-20727 a CVE-2024-20728 umožňujú zapisovať mimo povolené hodnoty v pamäti.

Zraniteľnosti CVE-2024-20729, CVE-2024-20731 a CVE-2024-20765 sa týkajú použitia dealokovaného miesta pamäte.

Chyba CVE-2024-20730 sa týka pretečenia celočíselnej premennej.

Úspešné zneužitie zraniteľností umožňuje ľubovoľné vykonávanie kódu.

Zraniteľné systémy:

Acrobat DC a Acrobat Reader DC pre Windows a Mac verzie 23.008.20470 a staršie,
Acrobat 2020 a Acrobat Reader 2020 pre Windows a Mac verzie 20.005.30539 a staršie.

Odporúčania:

Odporúčame aktualizáciu aspoň na verziu:
Acrobat DC a Acrobat Reader DC pre Windows a Mac 23.008.20533,
Acrobat 2020 a Acrobat Reader 2020 pre Windows a Mac 20.005.30574.

Zdroje:

https://helpx.adobe.com/security/security-bulletin.html
https://helpx.adobe.com/security/products/acrobat/apsb24-07.html

5. Frameworky

Microsoft .NET Framework

V mesiaci február spoločnosť Microsoft opravila 2 vysoko závažné zraniteľnosti vo frameworku .NET.

Vysoko závažné zraniteľnosti CVE-2024-21386 a CVE-2024-21404 môžu viesť k vyvolaniu nedostupnosti služby. Druhá v poradí zasahuje iba služby bežiace na iných platformách ako Windows.

Zraniteľné systémy:

ASP.NET Core 8.0
ASP.NET Core 7.0
ASP.NET Core 6.0
.NET 8.0
.NET 7.0
.NET 6.0

Zdroje:

https://portal.msrc.microsoft.com/en-us/security-guidance
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21386
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21404

Oracle Java

Veľká sada opráv je plánovaná na 16. apríla 2024.

Zdroje:

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

6. Iné závažné zraniteľnosti

Zraniteľnosti v Cisco

Spoločnosť Cisco poukázala na bezpečnostné chyby vo viacerých svojich produktoch. Tieto chyby umožňujú vzdialenému útočníkovi vykonávanie ľubovoľných príkazov a zvýšenie privilégií na úroveň root. **Viac informácií na stránke.**

Aktívne zneužívaná kritická zraniteľnosť FortiOS SSL VPN

Spoločnosť Fortinet vydala varovanie pred dvoma kritickými zraniteľnosťami. Obe kritické RCE zraniteľnosti umožňujú neautentifikovanému útočníkovi ľubovoľné vykonávanie kódu alebo príkazovprostredníctvom špeciálne vytvorených HTTP požiadaviek. Zraniteľnosť CVE-2024-21762 je aktívne zneužívaná. **Viac informácií na stránke.**

Ďalšia zero-day zraniteľnosť v produktoch Ivanti

Spoločnosť Microsoft vydala vo februári 2024 balík opráv pre operačné systémy Windows opravujúcich 73 zraniteľností, 5 z nich dostalo hodnotenie kritická. Dve zraniteľnosti sú typu zero-day. **Viac informácií na stránke.**

Kritická a zero-day zraniteľnosť v produktoch VMware

Spoločnosť CISA poukázala na aktívne zneužívanú kritickú zraniteľnosť (CVE-2023-34063), ktorá sa týka chýbajúcej kontroly prístupu a umožňuje získať neoprávnený prístup k vzdialeným organizáciam. Výskumník spoločnosti Trend Micro upozornil na zero-day zraniteľnosť (CVE-2023-34048) v produktoch VMware. Zneužitie zraniteľnosti umožňuje autentifikovanému útočníkovi vzdialené vykonávanie kódu. V súčasnosti je vystavených viac ako 2 000 serverov VMware Center týmto zraniteľnostiam. **Viac informácií na stránke.**

Kritická zraniteľnosť v GoAnywhere MFT

V produkte GoAnywhere Managed File Transfer (MFT) od spoločnosti Fortra bola nájdená bezpečnostná chyba. Úspešné zneužitie chyby umožňuje neautentifikovanému útočníkovi vytvoriť nového administrátorského používateľa systému. Celkovo 96,4% inštancií používa zraniteľnú verziu systému. **Viac informácií na stránke.**

Aktívne zneužívaná zero-day zraniteľnosť v Apple

Spoločnosť Apple vydala aktualizáciu pre zero-day zraniteľnosť CVE-2024-23222, ktorá môže viesť k vykonávaniu ľubovoľného kódu. Chyba je aktívne zneužívaná. **Viac informácií na stránke.**

Vysoko závažná zraniteľnosť v Splunk Enterprise

Spoločnosť Splunk vydala opravy zraniteľností v Splunk Enterprise vrátane chyby s vysokou závažnosťou, ktorá ovplyvňuje inštancie systému Windows. Úspešné zneužitie môže umožňovať odmietnutie služby alebo vykonávanie ľubovoľného kódu. **Viac informácií na stránke.**