Mesačný prehľad kritických zraniteľností
október 2023

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci október 12 kritických a 69 vysoko závažných zraniteľností.

Kritické zraniteľnosti CVE-2023-36697 a CVE-2023-35349 sa nachádzajú v službe Microsoft Message Queuing (MSMQ) a umožňujú vzdialené vykonávanie kódu (RCE). Pre ich zneužitie musí útočník presvedčiť obeť, aby sa pripojila ku škodlivému serveru alebo kompromitovať server, ku ktorému je pripojená. Microsoft na zmiernenie zraniteľností odporúča používateľom služby MSMQ skontrolovať, či je spustená a skontrolovať službu na porte TCP 1801.

Zraniteľnosti CVE-2023-38166, CVE-2023-41765, CVE-2023-41767, CVE-2023-41768, CVE-2023-41769, CVE-2023-41770, CVE-2023-41771, CVE-2023-41773 a CVE-2023-41774 sa nachádzajú v Layer 2 Tunneling protokole (L2TP). Pre ich zneužitie musí neautentifikovaný útočník vytvoriť špeciálnu požiadavku na pripojenie k RAS serveru, čo umožňuje vzdialené vykonávanie kódu.

Zraniteľnosť CVE-2023-36718 sa nachádza v module Microsoft Virtual Trusted Platform (vTPM) a umožňuje lokálnemu útočníkovi spustiť ľubovoľný kódu na cieľovom zariadení bez interakcie zo strany obete.

Vysoko závažné zraniteľnosti umožňujú obchádzanie bezpečnostných prvkov, eskaláciu oprávnení a narušenie dostupnosti služby. Zneužitie niektorých z nich môže viesť k úniku informácií a vzdialenému vykonávaniu kódu.

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 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)

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-2023-35349
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36697
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36718
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38166
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-41765
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-41767
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-41768
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-41769
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-41770
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-41771
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-41773
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-41774
https://nsfocusglobal.com/microsofts-october-security-update-for-multiple-high-risk-product-vulnerabilities/

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť opravila v mesiaci október 7 vysoko závažných zraniteľností.

Vysoko závažné zraniteľnosti CVE-2023-36565, CVE-2023-36568 a CVE-2023-36569 sa nachádzajú v Microsoft Office a úspešné zneužitie umožňuje zvýšenie oprávnení.

Zraniteľnosti CVE-2023-36780, CVE-2023-36789, CVE-2023-36786 a CVE-2023-41763 sa nachádzajú v aplikácii Skype for Business a umožňujú vzdialené vykonávanie kódu. Posledná môže viesť k eskalácii privilégií.

Zraniteľné systémy:

Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Office 2019 for 32-bit editions
Microsoft Office 2019 for 64-bit editions
Microsoft Office 2019 for Mac
Microsoft Office for Android
Microsoft Office for Universal
Microsoft Office LTSC 2021 for 32-bit editions
Microsoft Office LTSC 2021 for 64-bit editions
Microsoft Office LTSC for Mac 2021
Skype for Business Server 2015 CU13
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://msrc.microsoft.com/update-guide/en-us
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36569
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-41763
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36568
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36565
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36780
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36789
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36786

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 október 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 október neopravila v prehliadači Microsoft Edge žiadnu kritickú ani závažnú zraniteľnosť.

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

Mozilla Firefox
V mesiaci október boli opravené 3 vysoko závažné zraniteľnosti v línii Firefox a Firefox ESR.

Vysoko závažná zraniteľnosť CVE-2023-5721 sa týka nedostatočného oneskorenia aktivácie vyskakovacích okien a umožňuje zneužívanie kliknutia používateľa na spustenie akcie, ktorú nezamýšľal vykonať.

Zraniteľnosti CVE-2023-5730 (Firefox a Firefox ESR) a CVE-2023-5731 (Firefox) pokrývajú sadu zraniteľností ovplyvňujúcich bezpečnosť pamäte, ktoré môžu viesť ku poškodeniu pamäte alebo možnosti vykonávať kód.

Zraniteľné systémy:
Mozilla Firefox verzie staršie ako 119
Mozilla Firefox ESR verzie staršej ako 115.4

Odporúčania:

Odporúčame aktualizáciu Mozilla Firefox na verziu 119 a Mozilla Firefox ESR na verziu 115.4

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-45/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-46/

Google Chrome
V mesiaci október bola vydaná oprava 1 kritickej a 5 vysoko závažných zraniteľností prehliadača Google Chrome.

Kritická zraniteľnosť CVE-2023-5218 a vysoko závažná zraniteľnosť CVE-2023-5472 umožňuje použiť dealokované miesto v pamäti v komponentoch Site Isolation a Profiles.

Vysoko závažná zraniteľnosť CVE-2023-5480 sa týka nevhodnej implementácie vo funkcii platieb v komponente Payments.

Zraniteľnosti CVE-2023-5482 a CVE-2023-5849 sa nachádzajú v komponente USB API a týkajú sa nedostatočnej validácie údajov a pretečenia celočíselnej premennej. CVE-2023-5849

umožňuje vzdialenému útočníkovi spôsobiť poškodenie pamäte na halde prostredníctvom špeciálne vytvorenej stránky HTML.

CVE-2023-5346 sa nachádza v komponente V8 a súvisí s neoverením typu premennej.

Zraniteľné systémy:

Google Chrome pre Windows verzie staršej ako 119.0.6045.105/.106 a Linux a Mac verzie staršej ako 119.0.6045.105.

Odporúčania:

Odporúčame aktualizáciu prehliadača Chrome pre Windows aspoň na verziu 119.0.6045.105/.106 a Linux a Mac aspoň na verziu 119.0.6045.105.

Zdroje:

https://chromereleases.googleblog.com/2023/10/
https://chromereleases.googleblog.com/2023/10/stable-channel-update-for-desktop_24.html
https://chromereleases.googleblog.com/2023/10/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2023/10/stable-channel-update-for-desktop_10.html
https://chromereleases.googleblog.com/2023/10/stable-channel-update-for-desktop_31.html
https://www.suse.com/security/cve/CVE-2023-5849.html

4. Adobe Acrobat a Reader

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

Zdroje:

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

5. Frameworky

Microsoft .NET Framework

V mesiaci október spoločnosť Microsoft opravila 5 vysoko závažných zraniteľností vo frameworku .NET.

Závažné zraniteľnosti CVE-2023-36414 a CVE-2023-36415 sa nachádzajú v Azure Identity SDK for .NET a umožňujú vzdialené vykonávanie kódu.

Zraniteľnosti CVE-2023-38171, CVE-2023-36435 a CVE-2023-44487 sa nachádzajú v softvéri Microsoft QUIC a HTTP/2 protokole a môžu viesť k nedostupnosti služby.

Zraniteľné systémy:

.NET 6.0
.NET 7.0
ASP.NET Core 6.0
ASP.NET Core 7.0
Azure Identity SDK for .NET

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/en-us/security-guidance
https://nvd.nist.gov/vuln/detail/CVE-2023-36414
https://nvd.nist.gov/vuln/detail/CVE-2023-36415
https://nvd.nist.gov/vuln/detail/CVE-2023-38171
https://nvd.nist.gov/vuln/detail/CVE-2023-44487
https://nvd.nist.gov/vuln/detail/CVE-2023-36435

Oracle Java

V mesiaci október opravila spoločnosť Oracle v platforme Java SE a GraalVM Enterprise Edition 1 vysoko závažnú a 4 stredné zraniteľnosti.

Zraniteľnosť CVE-2023-30589 sa nachádza v komponente http, v systéme Node.js. Chýbajúca CRLF sekvencia ohraničovania umožňuje manipuláciu http požiadaviek.

CVE-2023-22067 umožňuje neautorizovanému útočníkovi s prístupom cez CORBA protokol, vkladať alebo mazať údaje v Oracle Java SE.

CVE-2023-22081 sa týka kompromitácie HTTPS a úspešné zneužitie môže viesť k odmietnutiu služby.

Úspešné zneužitie CVE-2023-22025 a CVE-2023-22091 môže viesť k neoprávnenému aktualizovaniu, mazaniu, vkladaniu alebo čítaniu údajov v Oracle Java SE a Oracle GraalVM.

Zraniteľné systémy:

Oracle Java SE: 8u381, 8u381-perf, 11.0.20, 17.0.8, 21; Oracle GraalVM for JDK: 17.0.8, 21; Oracle GraalVM Enterprise Edition: 20.3.11, 21.3.7, 22.3.3

Odporúčania:

Odporúčame aktualizáciu Oracle JavaSE a GraalVM Enterprise Edition na najnovšiu verziu.

Zdroje:

https://www.oracle.com/security-alerts/cpuoct2023.html
https://www.oracle.com/security-alerts/cpuoct2023verbose.html
https://access.redhat.com/security/cve/cve-2023-30589
https://www.suse.com/security/cve/CVE-2023-22067.html

6. Iné závažné zraniteľnosti

Čínska kyberšpionáž v produktoch Atlassian

Hackerská skupina podporovaná čínskou vládou aktívne zneužívala zero-day zraniteľnosť CVE-2023-22515 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.**

Kritické zraniteľnosti na CISCO zariadeniach

Spoločnosť Cisco upozornilo na aktívne zneužívanie dvoch zero-day zraniteľností. Napadnutých bolo viac ako 50 000 zariadení s operačným systémom IOS XE. Zraniteľnosti útočníkovi umožňujú zvýšenie práv na úroveň root. **Viac informácií na stránke.**

Microsoft opravil závažné zero-day zraniteľnosti

Spoločnosť Microsoft opravila 5 kritických a 2 zero-day zraniteľnosti vo viacerých svojich produktoch. Opravné aktualizácie boli vydané v rámci septembrového balíka Patch Tuesday. Zraniteľnosti umožňujú vzdialene vykonávať kód a získať oprávnenia na úrovni SYSTEM. **Viac informácií na stránke.**

Apple opravila 2 zero-day zraniteľnosti

Spoločnosť Apple vydala opravu dvoch zero-day zraniteľností CVE-2023-42824 a CVE-2023-5217, ktoré môžu viesť k eskalácii oprávnení a vzdialenému vykonávaniu kódu. Na kritickú zraniteľnosť CVE-2023-5217, ktorá sa týka pretečenia medzipamäte v komponente WebRTC, poukázala spoločnosť Google. Používateľom odporúčame nainštalovať si najnovšie dostupné aktualizácie. **Viac informácií na stránke.**

Zneužité kritické zraniteľnosti v aplikácii Zoho ManageEngine a FortiOS SSL-VPN

Spoločnosť CISA vydala varovanie ohľadom aktívneho zneužívania bezpečnostnej chyby v Zoho ManageEngine ServiceDesk Plus a Fortinet FortiOS SSL-VPN pre získanie neoprávneného prístupu do siete. Zraniteľnosti CVE-2022-47966 a CVE-2022-42475 umožňujú vzdialené vykonávanie kódu v spomenutých aplikáciách. **Viac informácií na stránke.**

Ďalšia Zero-Day zraniteľnosť prehliadača Google Chrome

Spoločnosť Google vydala bezpečnostnú aktualizáciu pre ďalšiu zero-day zraniteľnosť v prehliadačoch Chrome, Firefox, Brave a Edge. Kritická zraniteľnosť CVE-2023-4863 sa nachádza v komponente WebP a môže viesť k pádu aplikácie. **Viac informácií na stránke.**

Kritická zraniteľnosť v produktoch Adobe a Reader

Adobe vydala bezpečnostné aktualizácie na opravu zero-day zraniteľnosti v programe Acrobat a Reader a ďalšie vysoko závažné zraniteľnosti v Adobe Connect a Experience Manager. Zneužitie zraniteľností umožňuje útočníkovi vykonať útok typu Cross-Site Scripting (XSS), vykonávanie ľubovoľného kódu alebo dokonca poškodenie pamäte. **Viac informácií na stránke.**

Ďalšie zero-day zraniteľnosti v Apple

Spoločnosť Apple vydala opravu ďalších zero-day zraniteľností, ktoré môžu byť zreťazené a zneužité na útoky pomocou falošných SMS a WhatsApp správ. Zraniteľnosti CVE-2023-41991, CVE-2023-41992 a CVE-2023-41993 umožňujú útočníkovi obísť overenie certifikátu, zvýšiť oprávnenia a dosiahnuť vzdialené vykonávanie kódu. **Viac informácií na stránke.**