Mesačný prehľad kritických zraniteľností november 2022

1. Operačné systémy Microsoft Windows

Spoločnosť opravila v mesiaci november 7 kritické a 33 vysoko závažných zraniteľností.

Štyri opravené kritické zraniteľnosti umožňujú vzdialené vykonávanie kódu. CVE-2022-41039 a CVE-2022-41088 sa nachádzajú v protokole PPTP. Pre ich zneužitie musí útočník vytvoriť špeciálnu požiadavku na pripojenie k RAS serveru alebo odoslať PPTP serveru špeciálne vytvorený PPTP paket. CVE-2022-41118 a CVE-2022-41128 sa nachádzajú v skriptovacích jazykoch JScript9 a Chakra. Pre ich zneužitie musí útočník presvedčiť obeť, aby navštívila server aklebo webstránku, kde umiestnil škodlivý obsah.

Zraniteľnosti CVE-2022-37966 a CVE-2022-37967 sa nachádzajú v kryptografických komponentoch Kerberos a umožňujú získať vyššie oprávnenia až na úrovni administrátora.

Posledná kritická zraniteľnosť CVE-2022-38015 sa nachádza vo virtualizačnej platforme Hyper-V a umožňuje ovplyvniť dostupnosť služby.

Zraniteľnosti vysokej závažnosti umožňujú vzdialené vykonávanie kódu, eskaláciu oprávnení a obídenie bezpečnostných prvkov. 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 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 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 for ARM64-based Systems
Windows 11 for x64-based Systems
Windows 11 Version 22H2 for ARM64-based Systems
Windows 11 Version 22H2 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 2022 Datacenter: Azure Edition (Hotpatch)

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-2022-37966
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37967
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38015
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41039
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41088
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41118
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41128

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť opravila v mesiaci november 10 vysoko závažných zraniteľností a vydala jednu aktualizáciu pre zvýšenie bezpečnosti IRM zabezpečených dokumentov pre zaistenie dôveryhodnosti certifikačnej hierarchie.

Opravené zraniteľnosti CVE-2022-41061, CVE-2022-41107, CVE-2022-41063, CVE-2022-41106 a CVE-2022-41062 umožňujú vzdialené vykonávanie kódu. Zraniteľnosti CVE-2022-41103, CVE-2022-41060 a CVE-2022-41105 môžu viesť k úniku citlivých informácií. Zraniteľnosť CVE-

2022-41122 umožňuje predstierať cudziu identitu a CVE-2022-41104 dovoľuje obísť bezpečnostné prvky.

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 2013 RT Service Pack 1
Microsoft Word 2013 Service Pack 1 (32-bit editions)
Microsoft Word 2013 Service Pack 1 (64-bit editions)
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

3. Internetové prehliadače

Microsoft Internet Explorer

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

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

Microsoft Edge

Spoločnosť Microsoft v mesiaci november neopravila v prehliadači Microsoft Edge žiadnu kritickú ani vysoko závažnú zraniteľnosť.

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

Mozilla Firefox

V mesiaci november bolo opravených 8 vysoko závažných zraniteľností.

Zraniteľnosť CVE-2022-45403 umožňuje servisným pracovníkom odhadovať veľkosť mediálnych súborov z iných zdrojov.

Zraniteľnosť CVE-2022-45404 dovoľuje útočníkovi maximalizovať vyskakovacie okno prehliadača a podvrhnúť tak obeti podvodnú stránku. Podobné následky môže mať zraniteľnosť CVE-2022-45408, ktorá je spojená s opakovaným použitím hodnoty premennej „windowName“.

CVE-2022-45405 sa nachádza v implementácii rozhrania nsIInputStream, kde môže dôjsť k použitiu dealokovaného miesta v pamäti. Rovnaký typ zraniteľnosti je chyba v BaseShape

s označením CVE-2022-45406, ktorá nastáva pri vyčerpaní pamäte globálnej premennej JavaScriptu, pričom referencia na ňu zostáva aj po jej odstránení. K použitiu dealokovaného miesta môže dôjsť aj pri volaní fontu funkciou „FontFace()“. Táto chyba dostala označenie CVE-2022-45407. Poslednou zraniteľnosťou rovnakého typu je CVE-2022-45409, ktorá sa nachádza v „zberači odpadkov“. Vo viacerých stavoch a zónach môže nastať jeho prerušenie, pričom nedôjde k plánovanému volaniu funkcie „GCRuntime::finishCollection“.

Označenie CVE-2022-45421 pokrýva sadu zraniteľností ovplyvňujúcich bezpečnosť pamäte, ktoré môžu viesť ku poškodeniu pamäte alebo možnosti vykonávať kód.

Zraniteľné systémy:

Mozilla Firefox verzie staršie ako 105
Mozilla Firefox ESR verzie staršej ako 102.3

Odporúčania:

Odporúčame aktualizáciu Mozilla Firefox na verziu 105 a Mozilla Firefox ESR na verziu 102.3

Zdroje:

https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-47/

Google Chrome

V mesiaci november bola vydaná oprava 15 závažných zraniteľností prehliadača Google Chrome.

CVE-2022-4176 umožňuje zapisovať do pamäte mimo povolených hodnôt v komponente Lacros Graphics.

CVE-2022-3885, CVE-2022-3886, CVE-2022-3887, CVE-2022-3888, CVE-2022-4175, CVE-2022-4177, CVE-2022-4178, CVE-2022-4179, CVE-2022-4180 a CVE-2022-4181 umožňujú použiť dealokované miesto v pamäti v komponentoch V8, Speech Recognition, Web Workers, WebCodecs, Camera Capture, Extensions, Mojo, Audio a Forms.

CVE-2022-3890 a CVE-2022-4135 sú chyby pretečenia medzipamäte haldy v komponentoch Crashpad a GPU.

CVE-2022-3889 a CVE-2022-4174 súvisia s neoverením typu premennej v komponente V8.

Zraniteľné systémy:

Google Chrome pre Windows, Mac a Linux verzie staršej ako 106.0.5249.91.

Odporúčania:
Odporúčame aktualizáciu prehliadača Chrome pre Windows, Mac a Linux aspoň na verziu 106.0.5249.91.

Zdroje:
https://chromereleases.googleblog.com/2022/11/
https://chromereleases.googleblog.com/2022/11/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2022/11/stable-channel-update-for-desktop_24.html
https://chromereleases.googleblog.com/2022/11/stable-channel-update-for-desktop_29.html

4. Adobe Acrobat a Reader

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

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

5. Frameworky

Microsoft .NET Framework

V mesiaci november spoločnosť Microsoft opravila 1 vysoko závažnú zraniteľnosť vo frameworku .NET.

Zraniteľnosť s číslom CVE-2022-41064 môže viesť k úniku citlivých informácií. Útočník ju môže úspešne zneužiť po vyčerpaní všetkých dostupných výpočtových vlákien.

Zraniteľné systémy:

Microsoft .NET Framework 4.6.2
Microsoft .NET Framework 4.7 / 4.7.1 / 4.7.2
Microsoft .NET Framework 4.8 / 4.8.1

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-2022-41064

Oracle Java

Veľká sada opráv je plánovaná na 17. január 2023.

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

6. Iné závažné zraniteľnosti

Zero-day zraniteľnosti servera Microsoft Exchange

V produkte Microsoft Exchange a jeho súčasti Outlook Web App (OWA) boli objavené dve zraniteľnosti, pre ktoré aktuálne nie je dostupná bezpečnostná oprava, no existuje spôsob dočasnej opravy. Potenciálny vzdialený a autentifikovaný útočník by mohol zneužitím zraniteľností prevziať kontrolu nad serverom a nasadiť škodlivý webshell. Viac informácií na stránke.

Závažné zraniteľnosti v OpenSSL

V OpenSSL boli opravené dve vysoko závažné zraniteľnosti umožňujúce vyvolať nedostupnosť služby alebo v obmedzenej miere vykonávať vzdialene kód. Súvisia so spôsobom overovania e-mailových adries v certifikátoch X.509. Viac informácií na stránke.

Tri kritické zraniteľnosti VMware Workspace ONE dovolia obísť autentifikáciu

Spoločnosť VMware opravila tri kritické zraniteľnosti v produkte Workspace ONE, ktoré môže útočník zneužiť na získanie administrátorského prístupu ku zraniteľnej inštancii bez

autentifikácie. Viac informácií na stránke.

Kritické zraniteľnosti Citrix ADC a Gateway

Spoločnosť Citrix opravila tri kritické zraniteľnosti vo svojich produktoch ADC a Gateway. Útočníkom umožňujú obídenie autentifikácie a získanie kontroly nad zraniteľnou aplikáciou. Viac informácií na stránke.

Dve zraniteľnosti v F5 dovoľujú vzdialene vykonávať kód

V zariadeniach F5 BIG-IP a BIG-IQ sa nachádzajú dve zraniteľnosti vedúce k možnosti vzdialene vykonávať kód a získať kontrolu nad zraniteľným systémom. Spoločnosť F5 vydala hotfix a postup na ich mitigáciu. Viac informácií na stránke.

Chyba v Samba vedie k pretečeniu medzipamäte

V protokole Samba bola opravená chyba pretečenia medzipamäte na halde, ktorej zneužitie môže viesť k výpadku služby. Zraniteľnosť sa nachádza v knižniciach MIT Kerberos a Heimdal. Viac informácií na stránke.

Google opravil závažnú zero-day zraniteľnosť v Chrome

V prehliadači Chrome opravila spoločnosť Google zraniteľnosť vedúcu ku pretečeniu medzipamäte na halde. Hodnotená je ako vysoko závažná a je aktívne zneužívaná. Viac informácií na stránke.