Mesačný prehľad kritických zraniteľností
Október 2019

1. Operačné systémy Microsoft Windows

Spoločnosť opravila v mesiaci október 2 kritické zraniteľnosti.

Prvou opravenou kritickou zraniteľnosťou bola CVE-2019-1060. Táto zraniteľnosť vzniká, ak Microsoft XML Core Service (MSXML) spracováva vstupy používateľa. Po úspešnom zneužití zraniteľnosti dokáže útočník vzdialene vykonávať ľubovoľný kód a získať kontrolu nad zraniteľným systémom. Na zneužitie zraniteľnosti je potrebné, aby útočník hostil škodlivú stránku, ktorá dokáže spustiť MSXML cez webový prehliadač. Útočník musí presvedčiť používateľa, aby navštívil danú stránku, napríklad cez link v emailovej správe.

Kritická zraniteľnosť CVE-2019-1333 v operačnom systéme Windows sa nachádza v službe Remote Desktop Services. Útočníkovi umožňuje vzdialene vykonávať kód. Zneužiť zraniteľnosť je možné, ak útočník kontroluje server a používateľ sa naň pripojí. Presvedčiť používateľa môže pomocou sociálneho inžinierstva, otrávením DNS alebo vykonaním Man-in-the-middle útoku.

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 1703 for 32-bit Systems
Windows 10 Version 1703 for x64-based Systems
Windows 10 Version 1709 for 32-bit Systems
Windows 10 Version 1709 for 64-based Systems
Windows 10 Version 1709 for ARM64-based Systems
Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 1803 for ARM64-based Systems
Windows 10 Version 1803 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 1903 for 32-bit Systems
Windows 10 Version 1903 for ARM64-based Systems
Windows 10 Version 1903 for x64-based Systems
Windows 7 for 32-bit Systems Service Pack 1
Windows 7 for x64-based Systems Service Pack 1
Windows 8.1 for 32-bit systems
Windows 8.1 for x64-based systems
Windows RT 8.1

Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
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, version 1709 (Server Core Installation)
Windows Server, version 1903 (Server Core installation)
Windows Server, version 1803 (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-2019-1333
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1060

2. Kancelárske balíky Microsoft Office a Office Web Apps

V mesiaci október opravila spoločnosť Microsoft 6 závažných zraniteľností.

Medzi ne patrí zraniteľnosť vzdialeného vykonávania kódu CVE-2019-1331, CVE-2019-1327, ktorá je spôsobená tým, že Microsoft Excel nesprávne pracuje s objektami v pamäti. Na zneužitie môže útočník použiť špeciálne pripravený súbor. Potom musí ešte presvedčiť používateľa, aby tento súbor otvoril. To môže urobiť tak, že ho zašle pomocou e-mailu alebo rýchlej správy. Útočník môže taktiež využiť špeciálne vytvorenú stránku, pričom odkaz na ňu pošle používateľovi so snahou presvedčiť ho, aby ju navštívi. Po úspešnom zneužití tejto zraniteľnosti, môže útočník vykonávať akcie s právami aktuálne prihláseného používateľa.

Patrí tam aj cross-site scripting zraniteľnosť CVE-2019-1070, spoofing zraniteľnosť CVE-2019-1328, CVE-2019-1329 a CVE-2019-1330, ktoré umožňujú zvýšenie práv. Všetky štyri zraniteľnosti sa týkajú Microsoft SharePoint Servera.

Zraniteľné systémy:

Microsoft Excel 2010 Service Pack 2 (32-bit editions)
Microsoft Excel 2010 Service Pack 2 (64-bit editions)
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 2016 for Mac
Microsoft Office 2019 for 32-bit editions
Microsoft Office 2019 for 64-bit editions
Microsoft Office 2019 for Mac
Office 365 ProPlus for 32-bit Systems
Office 365 ProPlus for 64-bit Systems
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Server 2010 Service Pack 2
Microsoft SharePoint Server 2019

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-2019-1327
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1331
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1070
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1328
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1329
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1330

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft opravila v mesiaci október 2 kritické zraniteľnosti.

Zraniteľnosť CVE-2019-1238 a CVE-2019-1239, ktorá umožňuje vzdialené vykonávanie kódu, vzniká pri pristupovaní skriptovacieho nástroja VBScript ku objektom v pamäti. Útočník po zneužití zraniteľnosti získava rovnaké práva ako momentálne prihlásený používateľ. Ak je teda prihlásený administrátor, útočník môže získať kontrolu nad celým systémom. Na zneužitie tejto zraniteľnosti je potrebné hostiť webstránku, ktorej obsah je prispôsobený na využitie danej zraniteľnosti. Potom musí presvedčiť používateľa, aby navštívil danú stránku. Útočník môže takisto využiť kompromitované webové stránky alebo webové stránky, ktoré prijímajú alebo hostia obsah alebo reklamy poskytované používateľom na vloženie infikovaného obsahu. Naviac, môže útočník vložiť ovládací prvok ActiveX označený ako „bezpečný pre inicializáciu“ do aplikácie alebo dokumentu Microsoft Office.

Zraniteľné systémy:

Microsoft Internet Explorer verzie 10
Microsoft Internet Explorer verzie 11

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-2019-1238
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1239

Microsoft Edge

Spoločnosť Microsoft opravila tento mesiac 5 kritických zraniteľností.

Zraniteľnosť CVE-2019-1307, CVE-2019-1308, CVE-2019-1335, CVE-2019-1366, CVE-2019-1367 umožňuje vzdialené vykonávanie kódu, ak skriptovací nástroj Chakra nevhodne pristupuje ku objektom v pamäti. Na zneužitie tejto zraniteľnosti je potrebné hostiť webstránku, ktorej obsah je prispôsobený na zneužitie danej zraniteľnosti. Útočník potom musí presvedčiť používateľa, aby navštívil danú stránku. Takisto môže využiť kompromitované webové stránky alebo webové stránky, ktoré prijímajú alebo hostia obsah alebo reklamy poskytované používateľom. Útočník tak získava rovnaké práva ako momentálne prihlásený používateľ. Ak je teda prihlásený administrátor, útočník môže získať kontrolu nad celým systémom.

Zraniteľné systémy:

Microsoft Edge (EdgeHTML-based)v systémoch Windows 10 verzie 1809 v 32-bitových, 64-bitových verziách aj ARM64 verzii
Microsoft Edge (EdgeHTML-based) v systémoch Windows Server 2019
ChakraCore
Windows 10 Version 1709 for 32-bit Systems, x64-based Systems, ARM64-based Systems
Windows 10 Version 1803 for 32-bit Systems, x64-based Systems, ARM64-based Systems
Windows 10 Version 1903 for 32-bit Systems, x64-based Systems, for ARM64-based Systems
Windows 10 for 32-bit Systems, x64-based Systems
Windows 10 Version 1607 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Microsoft Edge (EdgeHTML-based) v systémoch Windows Server 2016
Windows 10 Version 1703 for 32-bit Systems, x64-based Systems

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-2019-1307
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1308
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1335
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1366
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1367

Mozilla Firefox

V mesiaci október boli opravené 4 závažné a 1 kritická zraniteľnosť.

Opravená bola kritická zraniteľnosť CVE-2019-11764, ktorá umožňuje vykonávať škodlivý kód a poškodiť pamäť.

Medzi závažné zraniteľnosti patrí zraniteľnosť s číslom CVE-2019-11758, ktorá vzniká pri inštalovaní programu 360 Total Security. Útočník dokáže poškodiť pamäť zariadenia a následne vykonať ľubovoľný kód. Medzi závažné zraniteľnosti tiež patrí CVE-2019-11757, ktorá je typu use-after-free (použitie už odalokovaného miesta v pamäti) a CVE-2019-15903, CVE-2019-6156, ktoré vznikajú pretečením haldy.

Zraniteľné systémy:
Mozilla Firefox verzia staršia ako 70
Mozilla Firefox ESR verzia staršia ako 68.2

Odporúčania:
Odporúčame aktualizáciu na novšie verzie.

Zdroje:
https://www.mozilla.org/en-US/seciurity/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-34/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-33/

Google Chrome

V októbri bola vydaná oprava na 45 zraniteľností, z toho je 8 závažných.

Prvou až piatou závažnou zraniteľnosťou je CVE-2019-13699, CVE-2019-13693, CVE-2019-13694, CVE-2019-13695, CVE-2019-13696, ktorá je typu use-after-free (opätovné použitie odalokovanej pamäte).
Ďalšie závažné zraniteľnosti sú CVE-2019-13697, CVE-2019-13700, CVE-2019-13701.

Zraniteľné systémy:
Google Chrome verzie staršie ako 78.0.3904.70

Odporúčania:
Odporúčame aktualizáciu na verziu 78.0.3904.70

Zdroje:
https://chromereleases.googleblog.com/2019
https://chromereleases.googleblog.com/2019/10/

4. Adobe Flash Player, Acrobat a Reader

Adobe Acrobat a Reader

Adobe zverejnil update pre Adobe Acrobat a Reader na operačných systémoch Windows, ktorý slúži na zabezpečenie kritických a závažných zraniteľností.

Opravených bolo 6 kritických zraniteľností, ktoré vznikajú pri zapisovaní do pamäte mimo hraníc. K nim patria zraniteľnosti CVE-2019-8171, CVE-2019-8186, CVE-2019-8165 a ďalšie. Závažná zraniteľnosť CVE-2019-8160 je typu cross-site scripting a pri nesprávnej

implementácií bezpečnostných mechanizmov vzniká zraniteľnosť CVE-2019-8226. Tieto zraniteľnosti môžu viesť ku vyzradeniu informácií.

CVE-2019-8164, CVE-2019-8168, CVE-2019-8172 a ďalších 18 závažných zraniteľností vzniká pri čítaní z pamäte mimo hraníc. Ďalších 26 zraniteľností je typu „use-after-free“ (používanie odalokovaného miesta v pamäti). Medzi nich patrí napríklad CVE-2019-8175, CVE-2019-8214 a CVE-2019-8176. Kritické zraniteľnosti CVE-2019-8170, CVE-2019-8183 a CVE-2019-8197 sú spôsobené pretečením haldy. CVE-2019-8166 vzniká pri chybe vo vyrovnávacej pamäti a CVE-2019-8162 pri race condition. Štyri kritické zraniteľnosti vznikajú pri nezhode typov a ďalšie štyri kritické zraniteľnosti sú spôsobené dereferenciou nedôveryhodného ukazovateľa. Každá z týchto zraniteľností umožňuje vykonávať ľubovoľný kód.

Zraniteľné systémy:

Acrobat DC 2019.012.20040 a staršie
Acrobat Reader DC 2019.012.20040 a staršie
Acrobat 2017.011.30148 a staršie
Acrobat Reader 2017.011.30148 a staršie
Acrobat 2015.006.30503 a staršie
Acrobat Reader 2015.006.30503 a staršie

Odporúčania:

Odporúčame používateľom aktualizovať softvér na najnovšiu verziu.

Zdroje:

https://helpx.adobe.com/security.html
https://helpx.adobe.com/security/products/acrobat/apsb19-49.html

5. Frameworky

Microsoft .NET Framework

Tento mesiac spoločnosť Microsoft nevydala žiadne aktualizácie opravujúce zraniteľnosti.

Zdroje:

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

Oracle Java

Spoločnosť Oracle vydala v mesiaci október plánovanú štvrťročnú veľkú sadu aktualizácií. V produkte Java SE a Java SE Embedded bolo celkovo opravených 30 zraniteľností. Prvé dve najdôležitejšie sú - CVE-2019-2949, CVE-2019-2989 so skóre 6.8.

Zraniteľné systémy:

Java SE: 7u231, 8u221, 11.0.4, 13;
Java SE Embedded: 8u221

Odporúčania:

Odporúčame aktualizovať zraniteľné verzie Java SE a Java SE Embedded na aktuálne verzie, prostredníctvom Java Auto Update alebo na stránke spoločnosti Oracle, viď prvý odkaz v zdrojoch.

Zdroje:

https://www.oracle.com/technetwork/topics/security/alerts-086861.html
https://www.oracle.com/security-alerts/cpuoct2019.html#AppendixJAVA

6. Iné

Spoločnosť Microsoft ponúka predĺženú podporu pre Windows 7

Koniec štandardnej technickej podpory pre Windows 7 bude v januári 2020, no spoločnosti môžu využívať podporu ESU. Ide o platenú špeciálnu podporu pre Windows 7 – Extended Security Updates. Pôvodne mala byť prístupná iba veľkým podnikom, tzv. Volume Licensing zákazníkom a okruhu používateľov Microsoft 365. Avšak, dostupná bude pre všetky spoločnosti, vzhľadom na to, že počas doby implementácie Windows 10 by boli dané spoločnosti nechránené. Ponuka platí pre edície Windows 7 Professional alebo Enterprise a malé podniky môžu využiť program Cloud Solution Provider. Podpora bude trvať do januára 2023.

Zdroje:

https://www.bleepingcomputer.com/news/microsoft/microsoft-to-offer-windows-7-extended-security-updates-to-smbs/
https://zive.aktuality.sk/clanok/142821/microsoft-rozsiruje-dostupnost-dodatocnej-podpory-pre-windows-7/