Mesačný prehľad kritických zraniteľností
December 2019

1. Operačné systémy Microsoft Windows

Spoločnosť opravila v mesiaci december dve kritické zraniteľnosti.

Opravená bola zraniteľnosť CVE-2019-1471, ktorá umožňuje útočníkovi vzdialene vykonávať kód. Vzniká, keď Windows Hyper-V na hostiteľskom serveri nesprávne vyhodnotí vstup od prihláseného používateľa na hosťovskom systéme. Ak útočník spustí na hosťovskom systéme špeciálne vytvorenú aplikáciu, môže vyvolať vykonanie ľubovoľného kódu v Hyper-V hostiteľskom systéme.

Druhou opravenou zraniteľnosťou bola CVE-2019-1468, ktorá umožňuje vzdialené vykonávanie kódu. Nachádza sa v knižnici fontov pri nevhodnom narábaní so špeciálne vytvorenými vloženými fontmi. Po zneužití zraniteľnosti dokáže útočník získať kontrolu nad systémom. Zneužiť zraniteľnosť je možné presvedčením používateľa, aby navštívil stránku, ktorá je upravená na zneužitie tejto zraniteľnosti alebo otvoriť špeciálne vytvorený súbor.

Opravených bolo aj 13 závažných zraniteľností.

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 1709 for 32-bit Systems
Windows 10 Version 1709 for ARM64-based Systems
Windows 10 Version 1709 for x64-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 10 Version 1909 for 32-bit Systems
Windows 10 Version 1909 for ARM64-based Systems
Windows 10 Version 1909 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 1803 (Server Core Installation)
Windows Server, version 1903 (Server Core installation)
Windows Server, version 1909 (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-2019-1471
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1468

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť opravila v mesiaci december 6 závažných zraniteľností. Štyri z nich, CVE-2019-1400 a CVE-2019-1463 (MS Access), CVE-2019-1464 (MS Excel) a CVE-2019-1491 (SharePoint Server) umožňujú únik citlivých údajov keď zraniteľný softvér nesprávne narába s objektmi v pamäti. Dve zraniteľnosti, CVE-2019-1461 a CVE-2019-1462 umožňujú vzdialené vykonávanie kódu nesprávnym narábaním s objektmi v pamäti.

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 2016
Microsoft SharePoint Foundation 2010 Service Pack 2
Microsoft SharePoint Foundation 2013 Service Pack 1
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-2019-1400
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1463
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1464
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1491
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1461
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1462

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft opravila tento mesiac jednu závažnú zraniteľnosť CVE-2019-1485. Zraniteľnosť 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 špeciálne pripravenú webstránku. Útočník 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 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-2019-1485

Microsoft Edge
Spoločnosť Microsoft tento mesiac v produkte MS Edge neopravila žiadne zraniteľnosti.

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

Mozilla Firefox
V mesiaci december bolo opravených 6 závažných zraniteľností.

Závažné zraniteľnosti CVE-2019-11756 a CVE-2019-17008 súvisia s použitím odalokovaného miesta v pamäti, CVE-2019-13722 súvisí s použitím nesprávneho množstva premenných vo WebRTC a vedie k porušeniu zásobníka v pamäti, CVE-2019-11745 dovoľuje zápis mimo povolených hraníc v pamäti v NSS pri šifrovaní blokovou šifrou. CVE-2019-17012 a CVE-2019-17013 sú chyby zabezpečenia pamäte, z ktorých môže časť viesť ku poruche pamäte s možnosťou vykonávať ľubovoľný kód.

Zraniteľné systémy:
Mozilla Firefox verzie staršie ako 71
Mozilla Firefox ESR verzie staršie ako 68.3

Odporúčania:
Odporúčame aktualizáciu na verziu 71 / ESR 68.3

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-36/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-37/

Google Chrome

V mesiaci december boli vydané opravy na 2 kritické a 9 závažných zraniteľností.

Kritická zraniteľnosť CVE-2019-13725 súvisí s použitím odalokovaného miesta v pamäti v komponente pre Bluetooth a CVE-2019-13726 s pretečením medzipamäte na halde v manažéri hesiel.

Zraniteľné systémy:

Google Chrome verzie staršie ako 79.0.3945.88

Odporúčania:

Odporúčame aktualizáciu na verziu 79.0.3945.88

Zdroje:

https://chromereleases.googleblog.com/2019
https://chromereleases.googleblog.com/2019/12/stable-channel-update-for-desktop_17.html
https://chromereleases.googleblog.com/2019/12/stable-channel-update-for-desktop.html

4. Adobe Flash Player, Acrobat a Reader

V mesiaci december vydala spoločnosť Adobe opravu 14 kritických a 7 závažných zraniteľností pre produkty Adobe Acrobat a Adobe Reader.

Všetky kritické zraniteľnosti môžu viesť k možnosti vykonávať ľubovoľný kód. CVE-2019-16450 a CVE-2019-164542 súvisia so zápisom do pamäte mimo povolené hodnoty; CVE-2019-16445, CVE-2019-16448, CVE-2019-16452, CVE-2019-16459 a CVE-2019-16464 s použitím odalokovaného miesta v pamäti; CVE-2019-16451 s pretečením haldy; CVE-2019-16462 s pretečením medzipamäte; CVE-2019-16446, CVE-2019-16455, CVE-2019-16460 a CVE-2019-16463 s dereferenciou nedôveryhodného ukazovateľa a CVE-2019-16453 s obchádzaním zabezpečenia.

6 závažných zraniteľností súvisí s čítaním mimo povolených hodnôt a môže viesť k úniku citlivých dát, zatiaľ čo jedna umožňuje eskaláciu práv.

Zraniteľné systémy:

Acrobat DC 2019. 021.20056 a staršie
Acrobat Reader DC 2019. 021.20056 a staršie

Acrobat 2017.011. 30152 a staršie (Windows)
Acrobat 2017.011. 30155 a staršie (macOS)
Acrobat Reader 2017.011. 30152 a staršie
Acrobat 2015.006.30505 a staršie
Acrobat Reader 2015.006.30505 a staršie

Odporúčania:
Odporúčame používateľom aktualizovať softvér na najnovšiu verziu.

Zdroje:
https://helpx.adobe.com/security.html
https://helpx.adobe.com/security.html#Bulletinsandadvisoriesbyproduct
https://helpx.adobe.com/security/products/acrobat/apsb19-55.html

5. Frameworky

Microsoft .NET Framework

V mesiaci december spoločnosť Microsoft nevydala žiadne opravné aktualizácie pre produkt .NET Framework.

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

Oracle Java

Veľká sada opráv je plánovaná na 14. januára 2020.

Zdroje:
https://www.oracle.com/technetwork/topics/security/alerts-086861.html

6. Iné závažné zraniteľnosti

Zraniteľnosť VPN v Linuxových a Unixových systémoch

Väčšina Linuxových distribúcií a Unixových systémov obsahuje zraniteľnosť, ktorá umožňuje útočníkom zistiť aktívne pripojenia do VPN, zistiť pripojenia na konkrétnu webstránku a injektovať ľubovoľné rámce do TCP prúdu. Viac informácií na našej stránke.