Mesačný prehľad kritických zraniteľností August 2019

1. Operačné systémy Microsoft Windows

Spoločnosť opravila v mesiaci august 16 kritických zraniteľností.

Zraniteľnosti CVE-2019-0720, CVE-2019-0965 umožňujú útočníkovi vykonávať ľubovoľný kód. Tieto zraniteľnosti vznikajú ak Windows Hyper-V Network Switch/ Windows Hyper-V na hostiteľskom serveri nesprávne vyhodnotí vstup od prihláseného používateľa na hosťovskom systéme. Ak útočník spustí na hosťovskom systéme vhodne vytvorenú aplikáciu, umožní mu to vykonávať ľubovoľný kód na hostiteľskom systéme.

Ďalšia kritická zraniteľnosť CVE-2019-0736, CVE-2019-1213 sa týka DHCP servera. Útočník môže poškodiť pamäť, ak pošle špeciálne upravené DHCP odpovede klientovi. Po zneužití dokáže vykonávať škodlivý kód na zariadení klienta.

Opravené boli aj zraniteľnosti CVE-2019-1144, CVE-2019-1145, CVE-2019-1149, CVE-2019-1150, CVE-2019-1151, CVE-2019-1152. Tieto zraniteľnosti vznikajú, ak knižnica fontov vo Windows nevhodne spracúva špeciálne upravené uložené fonty a umožňuje vzdialené vykonávanie kódu. Po zneužití zraniteľnosti môže útočník získať kontrolu nad zraniteľným systémom. Na napadnutie systému cez internet je potrebné, aby útočník hostil webovú stránku, ktorá je upravená na zneužitie tejto zraniteľnosti a aby presvedčil používateľa navštíviť ju (napríklad kliknutím na odkaz, ktorý na ňu smeruje). Napadnúť systém je možné aj cez zdieľanie dokumentu, ktorý je tiež upravený na zneužitie zraniteľnosti. Potom už len útočníkovi stačí presvedčiť používateľa, aby ho otvoril.

Kritické zraniteľnosti CVE-2019-1181, CVE-2019-1222, CVE-2019-1226, CVE-2019-1182 v operačnom systéme Windows / Windows Server sa nachádzajú v službe Remote Desktop Services. Neautorizovanému útočníkovi umožňujú bez interakcie používateľa vzdialene vykonávať kód a prevziať plnú kontrolu nad zraniteľným zariadením. Zneužiť sa dajú po zaslaní špeciálne upravenej požiadavky na cieľový systém Remote Desktop Service cez RDP.

Zraniteľnosť CVE-2019-1183, 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.

Ďalšia zraniteľnosť, ktorá umožňuje vzdialené vykonávanie kódu, je CVE-2019-1188. Vzniká pri spracovávaní súborov s príponou .LNK. Útočník po zneužití zraniteľnosti získava rovnaké práva ako momentálne prihlásený používateľ. Ak je teda prihlásený administrátor, útočník môže získať kontrolu nad celým systémom. Zneužiť zraniteľnosť útočník dokáže, keď používateľ otvorí napríklad vymeniteľné zariadenie, ktoré mu prezentuje útočník a v ktorom sa nachádza škodlivý kód. Po otvorení sa spustí daný kód a následne vie útočník vykonávať ľubovoľný kód na napadnutom zariadení.

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-2019-0720
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0965
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0736
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1144
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1145
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1149
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1150
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1151
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1152
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1181
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1213
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1222
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1226
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1182
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1183
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1188

2. Kancelárske balíky Microsoft Office a Office Web Apps

V mesiaci august opravila spoločnosť Microsoft 4 kritické zraniteľnosti.

Prvými dvomi opravenými zraniteľnosťami sú CVE-2019-1199 a CVE-2019-1200. Vznikajú, ak Microsoft Outlook nesprávne pracuje s objektmi v pamäti. Na zneužitie môže útočník použiť špeciálne pripravený súbor. Následne presvedčí 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, aby ho tak presvedčil nech ju navštívi. Po úspešnom zneužití tejto zraniteľnosti môže útočník vykonávať akcie s právami aktuálne prihláseného používateľa, napríklad vykonávať kód ako práve prihlásený používateľ.

Ďalšími opravený zraniteľnosťami sú CVE-2019-1201 a CVE-2019-1205. Vznikajú, ak Microsoft Word nesprávne pracuje s objektmi v pamäti. Na zneužitie môže útočník použiť špeciálne pripravený súbor. Následne musí presvedčiť používateľa, aby tento súbor otvoril. To môže urobiť tak, že zašle správu používateľovi pomocou e-mailu a počká, kým na ňu používateľ klikne. Správa sa zobrazí v Outlook Preview Pane cez Microsoft Word, čo spustí útok. Prípadne útočník priamo zašle upravený súbor cez e-mail a počká, kým ho používateľ otvorí. Útočník môže taktiež využiť špeciálne vytvorenú stránku, pričom odkaz na ňu pošle používateľovi. Po úspešnom zneužití tejto zraniteľnosti môže útočník vykonávať akcie s právami aktuálne prihláseného používateľa, napríklad vykonávať kód ako práve prihlásený používateľ.

Zraniteľné systémy:

Microsoft Office 2010 Service Pack 2 (32-bit editions)
Microsoft Office 2010 Service Pack 2 (64-bit editions)
Microsoft Office 2016 for Mac
Microsoft Office 2019 for 32-bit editions
Microsoft Office 2019 for 64-bit editions
Microsoft Office 2019 for Mac
Microsoft Office Online Server
Microsoft Office Web Apps 2010 Service Pack 2
Microsoft Office Web Apps Server 2013 Service Pack 1
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Server 2010 Service Pack 2
Microsoft SharePoint Server 2019
Microsoft Word 2010 Service Pack 2 (32-bit, 64-bit editions)
Microsoft Word 2013 RT Service Pack 1
Microsoft Word 2013 Service Pack 1 (32-bit, 64-bit editions)
Microsoft Word 2016 (32-bit edition)
Microsoft Word 2016 (64-bit edition)
Office 365 ProPlus for 32-bit Systems
Office 365 ProPlus for 64-bit 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. Pri zraniteľnosti CVE-2019-1201 je možné vypnúť funkciu Preview Pane, čo môže zmierniť útok.

Nesprávne používanie registračného editora (Registry Editor) môže viesť ku vážnym problémom. Je potrebné dôsledné preštudovanie problematiky.

Zdroje:
https://portal.msrc.microsoft.com/en-us/security-guidance
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1200
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1201
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1205
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1199

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft opravila v mesiaci august 2 kritické zraniteľnosti.

Zraniteľnosť CVE-2019-1133, CVE-2019-1194 umožňuje vzdialené vykonávanie kódu, ak skriptovací nástroj nevhodne pristupuje 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-2019-1133
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1194

Microsoft Edge

Spoločnosť Microsoft opravila tento mesiac 7 kritických zraniteľností.

Zraniteľnosť CVE-2019-1131, CVE-2019-1139, CVE-2019-1140, CVE-2019-1141, CVE-2019-1197, CVE-2019-1196, CVE-2019-1195 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 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. 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 v systémoch Windows 10 verzie 1809 v 32-bitových, 64-bitových verziách aj ARM64 verzii
Microsoft Edge 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 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-2019-1131
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1139
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1140
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1141
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1197
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1196
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1195

Mozilla Firefox

V mesiaci august bola opravená 1 stredne závažná zraniteľnosť.

Zraniteľnosť s číslom CVE-2019-11733 umožňuje zistiť uložené heslá z dialógu „Saved Logins“ bez toho, aby bolo zadané hlavné heslo.

Po nastavení hlavného heslo, je potrebné ho zadať opätovne, aby mal používateľ prístup k uloženým heslám. Zistilo sa, že lokálne uložené heslá je možné kopírovať do schránky prostredníctvom položky kontextovej ponuky „Kopírovať heslo“ bez opätovného zadania hlavného hesla. To môže potenciálne viesť ku krádeži hesiel.

Zraniteľné systémy:

Mozilla Firefox verzia staršia ako 68.0.2
Mozilla Firefox ESR verzia staršia ako 68.0.2

Odporúčania:

Odporúčame aktualizáciu na novšie verzie.

Zdroje:

https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-24/

Google Chrome

V auguste bola vydaná oprava na 7 zraniteľností, z toho sú 2 závažné.

Závažné zraniteľnosti CVE-2019-5869, CVE-2019-5868 vznikajú pri opätovnom použití odalokovanej pamäte (use-after-free).

Zraniteľné systémy:

Google Chrome verzie staršie ako 76.0.3809.132

Odporúčania:

Odporúčame aktualizáciu na verziu 76.0.3809.132

Zdroje:

https://chromereleases.googleblog.com/2019
https://chromereleases.googleblog.com/2019/08/stable-channel-update-for-desktop_26.html
https://chromereleases.googleblog.com/2019/08/stable-channel-update-for-desktop.html

4. Adobe Flash Player, Acrobat a Reader

Adobe Acrobat a Reader

Spoločnosť Adobe zverejnila aktualizáciu pre Adobe Acrobat a Reader na operačných systémoch Windows, ktorá slúži na zabezpečenie kritických a závažných zraniteľností.

Opravených bolo niekoľko závažných zraniteľností, ktoré vznikajú pri zapisovaní do pamäte mimo hraníc. K nim patria zraniteľnosti CVE-2019-8098, CVE-2019-8100, CVE-2019-7965 a ďalšie. Závažná zraniteľnosť CVE-2019-8060 vzniká pri zapisovaní príkazov. Ďalších 24 zraniteľností je typu „use-after-free“ (používanie odalokovaného miesta v pamäti). Medzi ne patrí napríklad CVE-2019-8003, CVE-2019-8024 a CVE-2019-8026. Zraniteľnosti CVE-2019-8066, CVE-2019-8050 a ďalšie sú spôsobené pretečením haldy. CVE-2019-8048 vzniká pri chybe vo vyrovnávacej pamäti, CVE-2019-8044 pri dvojnásobnom odalokovaní toho istého miesta v pamäti a CVE-2019-8019 pri nezhode typov. Závažné zraniteľnosti CVE-2019-8099 a CVE-2019-8101 vznikajú pri celočíselnom pretečení. Tri zraniteľnosti sú spôsobené dereferenciou nedôveryhodného ukazovateľa. Každá z týchto zraniteľností umožňuje vykonávať ľubovoľný kód.

Zraniteľnosti, ktoré môžu viesť k úniku informácií sú CVE-2019-8097, ktorá je spôsobená zverejnením interného IP, CVE-2019-8077, CVE-2019-8095, CVE-2019-8102 a ďalších 22, ktoré vznikajú pri čítaní z pamäte mimo hraníc.

Zraniteľné systémy:

Acrobat DC 2019.012.20035 a staršie
Acrobat Reader DC 2019.012.20035 a staršie
Acrobat DC 2017.011.30143 a staršie
Acrobat Reader 2017.011.30143 a staršie
Acrobat DC 2015.006.30498 a staršie
Acrobat Reader DC 2015.006.30498 a staršie

Odporúčania:

Vzhľadom na počet opravených zraniteľností odporúčame používateľom aktualizovať softvér na najnovšiu verziu.

Zdroje:

https://helpx.adobe.com/security.html
https://helpx.adobe.com/security/products/acrobat/apsb19-41.html

5. Frameworky

Microsoft .NET Framework

Tento mesiac spoločnosť Microsoft nevydala žiadne aktualizácie opravujúce zraniteľnosti .NET Framework.

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

Oracle Java

Veľká sada opráv je plánovaná 15. októbra 2019.

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

6. Iné závažné zraniteľnosti

Desiatky ovládačov pre Windows umožňujú ovládnuť systém

Výskumníci spoločnosti Eclypsium študovali vyše 40 ovládačov od 20 spoločností. Objavili v nich zraniteľnosti vedúce ku zvýšeniu práv a k možnosti čítať a zapisovať do systémovej pamäte a registrov. Takto môžu útočníci vykonávať kód so systémovými právami, či zasahovať do firmvéru. Na zraniteľnom zariadení dokážu získať perzistenciu a kompletne ho ovládnuť.

Viac informácií na stránke.

QualPwn - Ako ovládnuť Android zariadenie pomocou zraniteľností čipov Qualcomm

Bezpečnostný tím Blade spoločnosti Tencent našiel tri zraniteľnosti súhrnne označené ako QualPwn, nachádzajúce sa v čipoch Qualcomm, využívaných v zariadeniach Android. Útočníkom s prístupom na WLAN, ku ktorej je pripojené zraniteľné zariadenie, umožňujú na tomto zariadení vykonávať kód a prevziať nad ním kontrolu. Útok si nevyžaduje interakciu používateľa.

Viac informácií na stránke.