Mesačný prehľad kritických zraniteľností
November 2019

1. Operačné systémy Microsoft Windows

Spoločnosť opravila v mesiaci november 8 kritických zraniteľností.

Zraniteľnosti CVE-2019-1397, CVE-2019-1389, CVE-2019-0721, CVE-2019-0719, CVE-2019-1398, 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.

Zraniteľnosť CVE-2019-1419 vzniká, ak Windows knižnica Adobe Type Manager Library nevhodne spracuje špeciálne upravené OpenType fonty. Po zneužití zraniteľnosti dokáže útočník vzdialene vykonávať kód, ak ide o iný operačný systém ako Windows 10. Pri Windows 10, dokáže útočník spustiť kód v AppContainer kontexte s obmedzenými právami. Na zneužitie zraniteľnosti musí útočník presvedčiť používateľa, aby otvoril špeciálne upravený dokument alebo aby navštívil stránku, ktorá používa upravené zraniteľné fonty.

Ďalšou zraniteľnosťou, ktorá umožňuje vzdialene vykonávať kód je CVE-2019-1430. Vzniká ak Windows Media Foundation nevhodne spracováva špeciálne upravené QuickTime súbory. Útočník po zneužití získava rovnaké práva ako lokálny používateľ. Na zneužitie je potrebné, aby bol používateľovi doručený upravený QuickTime súbor a následne otvorený používateľom.

Zraniteľnosť CVE-2019-1441 sa tiež týka fontov a ich nevhodným spracovaním. Taktiež umožňuje útočníkovi vzdialene vykonávať kód. 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 súbor, ktorý dokáže danú zraniteľnosť zneužiť.

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-2019-1397
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1389
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0721
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0719
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1398
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1419

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1430
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1441

2. Kancelárske balíky Microsoft Office a Office Web Apps

V mesiaci november bolo opravených aj viacero závažných zraniteľností.

Medzi nich patrí zraniteľnosť CVE-2019-1402 v Microsoft Office, keď softvér nevhodne pristupuje ku objektom v pamäti. Zraniteľnosť CVE-2019-1443 v Microsoft SharePoint, pri ktorej môže dôjsť k úniku informácií. Ako aj pri CVE-2019-1446 v Microsoft Excel softvéri. Ak Microsoft Office nesprávne overí URL adresu, môže dôjsť ku obídeniu bezpečnostnej kontroly – zraniteľnosť CVE-2019-1442. Ďalšou zraniteľnosťou je CVE-2019-1448, ktorá je spôsobená tým, že Microsoft Excel nesprávne pracuje s objektami v pamäti. Opravené boli aj ďalšie zraniteľnosti.

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 2010 Service Pack 2 (32-bit editions)
Microsoft Office 2010 Service Pack 2 (64-bit editions)
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 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-2019-1402
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1443
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1446
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1442

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft opravila v mesiaci november 2 kritické zraniteľnosti.

Zraniteľnosť CVE-2019-1390, 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.

Zraniteľnosť CVE-2019-1429 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 zneužitie danej zraniteľnosti. Potom musí útočník 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-2019-1390
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1429

Microsoft Edge
Spoločnosť Microsoft opravila tento mesiac 3 kritické zraniteľnosti.

Zraniteľnosť CVE-2019-1428, CVE-2019-1427 a CVE-2019-1426 umožňuje vzdialené vykonávanie kódu, ak skriptovací nástroj 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 (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-2019-1428
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1427
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1426

Mozilla Firefox
V mesiaci november neboli opravené žiadne zraniteľnosti.

Zdroje:
https://www.mozilla.org/en-US/seciurity/advisories/

Google Chrome
V októbri bola vydaná oprava na 8 zraniteľností, z toho sú 2 závažné.

Zraniteľnosť CVE-2019-13723 je typu use-after-free (opätovné použitie odalokovanej pamäte) a CVE-2019-13724 vzniká pri pristupovaní do systému mimo povolených hodnôt. Obe súvisia s prístupom k Bluetooth.

Zraniteľné systémy:
Google Chrome verzie staršie ako 78.0.3904.106

Odporúčania:
Odporúčame aktualizáciu na verziu 78.0.3904.106

Zdroje:
https://chromereleases.googleblog.com/2019
https://chromereleases.googleblog.com/2019/11/stable-channel-update-for-chrome-os_19.html
https://chromereleases.googleblog.com/2019/11/stable-channel-update-for-desktop_18.html

4. Adobe Flash Player, Acrobat a Reader

V mesiaci november nevydala spoločnosť Adobe žiadne opravy pre Flash Player, Acrobat a Reader.

Zdroje:
https://helpx.adobe.com/security.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 na 14. januára 2020.

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

6. Iné

Kritická zneužívaná zraniteľnosť v PHP-FPM umožňuje vzdialene vykonávať kód

V PHP7 bola opravená kritická zraniteľnosť súvisiaca s podtečením premennej, ktorá umožňuje vzdialene vykonávať ľubovoľný kód. Zraniteľnosť je zneužiteľná na nginx serveroch, ktoré súčasne využívajú prostredie PHP-FPM. Výskumníci zverejnili funkčnú

ukážku jej zneužitia a zraniteľnosť je aktuálne reálne zneužívaná. Odporúčame bezodkladnú aktualizáciu PHP, alebo aspoň vykonanie zmierňujúcich opatrení. Viac informácií na stránke.

Kritická zero-day zraniteľnosť Google Chrome umožňuje vzdialene vykonávať kód

Dňa 31.10.2019 bola publikovaná oprava kritickej zero-day zraniteľnosti v prehliadači Google Chrome, konkrétne v jeho audio komponente, umožňujúcej použiť odalokované miesto v pamäti. Bolo zaznamenané aktívne zneužitie tejto zraniteľnosti útočníkmi. Súčasne bola opravené podobná zraniteľnosť v komponente prehliadača PDFium. Viac informácií na stránke.

Kritické zraniteľnosti v nástroji rConfig umožňujú vzdialene vykonávať kód

Sieťový nástroj rConfig obsahuje dve zraniteľnosti umožňujúce vzdialene vykonávať systémové príkazy, čo môže viesť ku vzdialenému vykonávaniu kódu. Jedna zo zraniteľností je hodnotená ako kritická, nakoľko jej zneužitie nevyžaduje autentifikáciu útočníka. Nástroj sa momentálne javí ako nepodporovaný, preto sa odporúča nepoužívať ho. Viac na stránke.

Intel opravil 77 zraniteľností, niektoré na hardvérovej úrovni

Spoločnosť Intel vydala opravy 77 zraniteľností v širokej škále svojich produktov vrátane procesorov, grafických čipov a sieťových kariet. Niekoľko z nich je hodnotených ako kritické a závažné. Umožňujú najmä únik citlivých dát a zvýšenie práv. Jednou z nich je nová zraniteľnosť súvisiaca s technológiou špekulatívnej exekúcie a umožňujúca únik citlivých údajov cez postranný kanál. Dostala názov ZombieLoad 2 a postihuje tiež niektoré procesory imúnne voči RIDL a Fallout. Viac informácií tu.