Mesačný prehľad kritických zraniteľností
September 2019

1. Operačné systémy Microsoft Windows

Spoločnosť opravila v mesiaci september 5 kritických zraniteľností.

Kritická zraniteľnosť CVE-2019-0787, CVE-2019-0788, CVE-2019-1290, CVE-2019-1291 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, pomocou útoku typu DNS poisoning, alebo vykonaním Man-in-the-middle útoku.

Ďalšia zraniteľnosť, ktorá umožňuje vzdialené vykonávanie kódu, je CVE-2019-1280. 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-2019-0787
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0788
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1290
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1280
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1291

2. Kancelárske balíky Microsoft Office a Office Web Apps

V mesiaci september opravila spoločnosť Microsoft 3 kritické zraniteľnosti.

Prvou a druhou opravenou zraniteľnosťou je CVE-2019-1295, CVE-2019-1296, ktoré umožňujú vzdialené vykonávanie kódu v kontexte danej SharePoint aplikácie a SharePoint servera. Vznikajú pri nedostatočnom zabezpečení APIs SharePointu pred nebezpečnými vstupmi. Na zneužitie týchto zraniteľností je potrebné, aby používateľ zadal do API v zraniteľnej verzii SharePointu špeciálne naformátovaný vstup.

Treťou zraniteľnosťou je CVE-2019-1306. Vzniká, ak Azure DevOps Server(ADO) a Team Foundation Server(TFS) nesprávne overí vstupné dáta. Na zneužitie danej zraniteľnosti je potrebné, aby útočník uploadol špeciálne upravený súbor na ADO a TFS Server a počkal, kým priradí k súboru index. Potom môže útočník vykonať ľubovoľný súbor s právami práve prihláseného používateľa.

Zraniteľné systémy:

Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Server 2010 Service Pack 2
Microsoft SharePoint Server 2019
Azure DevOps Server 2019 Update 1
Azure DevOps Server 2019.0.1
Team Foundation Server 2018 Update 3.2

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-2019-1296
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1295
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1306

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft opravila v mesiaci september 4 kritické zraniteľnosti.

Zraniteľnosť CVE-2019-1367, CVE-2019-1221 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.

Zraniteľnosť CVE-2019-1208, CVE-2019-1236, 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-2019-1367
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1221
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1208
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1236

Microsoft Edge

Spoločnosť Microsoft opravila tento mesiac 5 kritických zraniteľností.

Zraniteľnosť CVE-2019-1237, CVE-2019-1138, CVE-2019-1217, CVE-2019-1298, CVE-2019-1300 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(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-2019-1237
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1138
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1217
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1298
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1300

Mozilla Firefox

V mesiaci september bolo opravených 10 závažných a 1 kritická zraniteľnosť.

Opravená bola kritická zraniteľnosť CVE-2019-11751, ktorá umožňuje vykonávať škodlivý kód cez príkazový riadok. Vzniká, ak nie sú parametre v príkazovom riadku správne spracované a iným program spustí Firefox.

Medzi závažné zraniteľnosti patrí zraniteľnosť s číslom CVE-2019-11740, po ktorej zneužití dokáže útočník poškodiť pamäť a vykonať ľubovoľný kód, CVE-2019-11752, ktorá je typu use-after-free(použitie už odalokovaného miesta v pamäti), CVE-2019-11744, ktorá umožňuje vykonať cross-site scripting útok a ďalšie.

Zraniteľné systémy:

Mozilla Firefox verzia staršia ako 69.0.1
Mozilla Firefox ESR verzia staršia ako 68.1

Odporúčania:
Odporúčame aktualizáciu na novšie verzie.

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-27/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-26/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-25/

Google Chrome

V septembri bola vydaná oprava na 56 zraniteľností, z toho sú 2 kritické a 11 závažných.

Medzi kritické zraniteľnosti patria CVE-2019-5870 a CVE-2019-13685, ktoré sú typu use-after-free (opätovné použitie odalokovanej pamäte).
Niektoré závažné zraniteľnosti ako napríklad CVE-2019-5872, CVE-2019-5873 a CVE-2019-13687 sú tiež typu use-after-free. CVE-2019-5871 vzniká pri pretečení haldy.

Zraniteľné systémy:
Google Chrome verzie staršie ako 77.0.3865.90

Odporúčania:
Odporúčame aktualizáciu na verziu 77.0.3865.90

Zdroje:
https://chromereleases.googleblog.com/2019
https://chromereleases.googleblog.com/2019/09/stable-channel-update-for-desktop_18.html
https://chromereleases.googleblog.com/2019/09/stable-channel-update-for-desktop.html

4. Adobe Flash Player, Acrobat a Reader

Adobe Flash Player

Adobe zverejnil update pre Adobe Flash Player na operačných systémoch Windows, ktorý slúži na zabezpečenie kritických zraniteľností.

Opravené boli 2 kritické zraniteľnosti. Prvá CVE-2019-8070 vzniká pri používaní odalokovaného miesta v pamäti „use-after-free“. Druhá CVE-2019-8069 vzniká pri spustení metódy toho istého pôvodu. Obe z týchto zraniteľností umožňujú vykonávať ľubovoľný kód.

Zraniteľné systémy:
Adobe Flash Player Desktop Runtime 32.0.0.238 a staršie
Adobe Flash Player for Google Chrome 32.0.0.238 a staršie
Adobe Flash Player for Microsoft Edge and Internet Explorer 11 32.0.0.207 a staršie

Odporúčania:
Odporúčame používateľom aktualizovať softvér na najnovšiu verziu.

Zdroje:
https://helpx.adobe.com/security.html
https://helpx.adobe.com/security/products/flash-player/apsb19-46.html

5. Frameworky

Microsoft .NET Framework
Tento mesiac vydala spoločnosť Microsoft opravu na 1 kritickú zraniteľnosť.

Zraniteľnosť CVE-2019-1142 vzniká, ak .NET Framework common language runtime(CRL) umožní vytvorenie súboru v ľubovoľnom priečinku. Po úspešnom zneužití zraniteľnosti dokáže útočník zapisovať súbory do priečinkov, ktoré vyžadujú vyššie privilégia ako daný útočník má. Na zneužitie je potrebné byť prihlásený do systému, špecifikovať cieľový priečinok a spustiť škodlivý proces.

Zraniteľné systémy:
Microsoft .NET Framework 3.5
Microsoft .NET Framework 4.7.2
Microsoft .NET Framework 4.8
Microsoft .NET Framework 4.5.2
Microsoft .NET Framework 4.7.1
Microsoft .NET Framework 4.7
Microsoft .NET Framework 4.6
Microsoft .NET Framework 4.6.1
Microsoft .NET Framework 4.6.2

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-2019-1142

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

Kritická zero-day zraniteľnosť v Microsoft Internet Explorer umožňuje vzdialene vykonávať kód

Dňa 23.9.2019 spoločnosť Microsoft mimoriadne vydala opravu kritickej zero-day zraniteľnosti v softvéroch Internet Explorer 9, 10 a 11, ktorá útočníkovi umožňuje vzdialené vykonanie ľubovoľného kódu. Zraniteľnosť je útočníkmi aktívne zneužívaná. Útočník môže pomocou špeciálne pripravenej škodlivej stránky zneužiť chybu v správe objektov v pamäti v skriptovacom nástroji. Následne dôjde ku narušeniu integrity pamäte, čo možno zneužiť na vzdialené vykonanie ľubovoľného škodlivého kódu s právami práve prihláseného používateľa. Útočník musí nalákať používateľa na návštevu danej stránky.

Viac informácií na stránke.

WordPress 5.2.3 opravuje množstvo chýb

Vývojári CMS Wordpress vydali novú verziu 5.2.3, ktorá obsahuje 29 vylepšení a opráv. Okrem iného boli odstránené mnohé zraniteľnosti v rôznych komponentoch platformy, umožňujúce XSS útoky. Niektoré závažné zraniteľnosti mohli viesť tiež ku vzdialenému vykonávaniu kódu. Vývojári aktualizovali aj komponent jQuery v starších verziách, kvôli závažnej zraniteľnosti umožňujúcej XSS útoky.

Viac informácií na stránke.

NetCAT - Útok na procesory od Intelu

Bezpečnostní výskumníci z Vrije University v Amsterdame objavili zraniteľnosť v procesoroch od spoločnosti Intel využívajúcich technológie DDIO (Data Direct I/O) a RDMA (Remote Direct Memory Access). Zraniteľnosť demonštrovali zachytením hesla pre SSH pripojenie počas toho, ako ho používateľ zadáva pomocou klávesnice. Je možné ju zneužiť bez toho, aby mal útočník fyzický prístup ku zariadeniu a taktiež bez predchádzajúcej inštalácie malvéru. Zraniteľnosť nájdeme pod číslom CVE-2019-11184.

Viac informácií na stránke.

Zraniteľné CISCO produkty umožňujú prevzatie kontroly nad systémom

Výskumník Pedro Ribeiro našiel 3 závažné až kritické zraniteľnosti v produktoch od spoločnosti Cisco. Po zneužití týchto zraniteľností môže útočník získať kontrolu nad zraniteľným systémom. Okrem daných troch zraniteľností bolo opravených aj ďalších 14 vysoko závažných a kritických zraniteľností. Dané zraniteľnosti sa týkajú UCS produktov (Unified Computing System Products), vrátane Integrated Management Controller (IMC), UCS Director a UCS Director Express pre veľké dáta (Big Data).

Viac informácií na stránke.