Mesačný prehľad kritických zraniteľností
Jún 2019

1. Operačné systémy Microsoft Windows

Spoločnosť opravila v mesiaci jún 5 kritických zraniteľností.

Zraniteľnosti CVE-2019-0620, CVE-2019-0709, CVE-2019-0722 umožňujú útočníkovi vykonávať ľubovoľný kód. Tieto zraniteľnosti vznikajú ak 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.

Opravená bola aj kritická zraniteľnosť CVE-2019-0888. Vzniká pri pristupovaní ActiveX Data Objects (ADO) ku objektom v pamäti. Ak útočník zneužije zraniteľnosť, je schopný vykonávať ľubovoľný kód s používateľskými právami. Na úspešné zneužitie je potrebné vytvoriť webovú stránku, ktorá dokáže zneužiť zraniteľnosť a potom presvedčiť používateľa, aby ju navštívil.

Ďalšou opravenou zraniteľnosťou bola CVE-2019-0985, ktorá umožňuje útočníkovi vykonávať ľubovoľný kód. Vzniká, ak Microsoft Speech API (SAPI) nevhodne spracuváva „text-to-speech“ vstupy. Na zneužitie zraniteľnosti je potrebné, aby útočník presvedčil používateľa, aby otvoril špeciálne upravený súbor, ktorý obsahuje „text-to-speech“ obsah.

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-2019-0722
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0709
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0620
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0888
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0985

2. Kancelárske balíky Microsoft Office a Office Web Apps

Tento mesiac bola vydaná oprava iba na závažné zraniteľnosti.

Zraniteľnosti CVE-2019-0904 – CVE-2019-0909, CVE-2019-0974 sú spôsobené nesprávnym spracovaním objektov v pamäti aplikáciou Windows Jet Database Engine. Útočník môže využiť špeciálne pripravený súbor a po úspešnom zneužití získa možnosť vykonávať ľubovoľný kód.

Zraniteľné systémy:
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 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.

Zdroje:
https://portal.msrc.microsoft.com/en-us/security-guidance
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0904
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0905
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0906
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0907
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0908
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0909
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0974

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft opravila v mesiaci jún 3 kritické zraniteľnosti.

Zraniteľnosť CVE-2019-0920, CVE-2019-0988 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.

Zraniteľnosť CVE-2019-1038 vzniká pri pristupovaní prehliadačov ku objektom v pamäti. Na zneužitie zraniteľnosti útočník môže hostiť webstránku, ktorej obsah je prispôsobený na využitie tejto zraniteľnosti cez Internet Explorer. Potom sa mu musí podariť presvedčiť používateľa, aby otvoril škodlivú webstránku. Útočník môže takisto využiť kompromitované webové stránky alebo webové stránky, ktoré prijímajú alebo hostia obsah alebo reklamy poskytované používateľom na pridanie infikovaného súboru. Niekedy sa od používateľa očakáva aktívny prístup (kliknutie na odkaz,..). Zneužitie tejto zraniteľnosti umožňuje vzdialené vykonávanie kódu. Útočník získava rovnaké práva ako prihlásený používateľ. Ak je prihlásený administrátor, útočník získa práva administrátora a získa kontrolu nad celým systémom.

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-2019-0920

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0988

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1038

Microsoft Edge

Spoločnosť Microsoft opravila tento mesiac 13 kritických zraniteľností.

Zraniteľnosť CVE-2019-0991 – CVE-2019-0993, CVE-2019-1002, CVE-2019-1003, CVE-2019-1024, CVE-2019-1051, CVE-2019-1052, CVE-2019-1055 a CVE-2019-1080 a CVE-2019-0989 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.

Ďalšia kritická zraniteľnosť CVE-2019-1023, CVE-2019-0990 vzniká taktiež, ak skriptovací nástroj nevhodne pristupuje ku objektom v pamäti a na zneužitie je potrebné vykonať

rovnaké kroky ako pri predchádzajúcich zraniteľnostiach, no po zneužití dostáva útočník prístup ku informáciám používateľa, ktoré môže následne použiť na kompromitovanie systému.

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-2019-0990
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0991
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0992
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0993
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1002
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1003
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1051
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1052
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1023
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1024
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1080
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1055
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0989

Mozilla Firefox

V mesiaci jún bola opravená 1 kritická a 1 závažná zraniteľnosť.

Kritická zraniteľnosť CVE-2019-11707 vzniká pri manipulácií s objektmi JavaScript. Táto zraniteľnosť je typu „type confusion“ (chyba dátových typov).

Závažná zraniteľnosť CVE-2019-11708 umožňuje vykonávanie ľubovoľného kódu. Nedostatočná kontrola parametrov odovzdaná s výzvou „Otvorená IPC správa“ medzi detským a rodičovským procesom, môže viesť ku otvoreniu webového obsahu, ktorý vybral skompromitovaný detský proces.

Zraniteľné systémy:

Mozilla Firefox verzie staršie ako 67.0.3 / ESR 60.7.1

Odporúčania:

Odporúčame aktualizáciu na verziu 67.0.3 / ESR 60.7.1

Zdroje:

https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-18/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-19/

Google Chrome

V mesiaci jún bola vydaná oprava na 43 zraniteľností.

Z toho boli 3 zraniteľnosti závažné. CVE-2019-5828, CVE-2019-5829 a CVE-2019-5842 sú typu „use after free“ (použitie už odblokovaného miesta v pamäti).

Zraniteľné systémy:

Google Chrome verzie staršie ako 75.0.3770.80

Odporúčania:

Odporúčame aktualizáciu na verziu 75.0.3770.80

Zdroje:

https://chromereleases.googleblog.com/2019
https://chromereleases.googleblog.com/2019/06/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2019/06/stable-channel-update-for-desktop_13.html

https://chromereleases.googleblog.com/2019/06/stable-channel-update-for-chrome-os-m75.html

4. Adobe Flash Player, Acrobat a Reader

Adobe Flash Player

Pre Adobe Flash Player bola zverejnená aktualizácia opravujúca kritickú zraniteľnosť CVE-2019-7845. Táto zraniteľnosť je typu „use-after-free“, (používanie odalokovaného miesta v pamäti) a umožňuje vykonávanie ľubovoľného kódu.

Zraniteľné systémy:
Adobe Flash Player Desktop Runtime 32.0.0.192 a staršie
Adobe Flash Player for Google Chrome 32.0.0.192 a staršie
Adobe Flash Player for Microsoft Edge and Internet Explorer 11 32.0.0.192 a staršie

Odporúčania:
Spoločnosť Adobe odporúča používateľom aktualizovať systémy na verziu 32.0.0.207.

Zdroje:
https://helpx.adobe.com/security.html
https://helpx.adobe.com/security/products/flash-player/apsb19-30.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

Najbližšia veľká sada aktualizácií je plánovaná na 16.júla 2019.

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

6. Iné závažné zraniteľnosti

Zraniteľnosti v prehrávači VLC Media Player umožňujú prevziať kontrolu nad počítačom

Multimediálny prehrávač VLC Media Player, ktorý používajú stovky miliónov používateľov, mal dve závažné zraniteľnosti, ktoré umožňovali útočníkom vzdialene vykonávať ľubovoľný kód na zraniteľnom systéme a prevziať nad ním úplnú kontrolu. Zraniteľné verzie VLC Player je možné zneužiť pomocou špeciálne upraveného súboru MKV, alebo AVI, ktorý používateľ spustí po stiahnutí, alebo streamuje z internetu. Viac informácií na stránke.

Spam s dva roky starou zraniteľnosťou MS Office šíri malvér

Spoločnosť Microsoft varuje pred novou kampaňou útokov, ktorá bola nedávno spustená. Útočníci zneužívajú chybu v kancelárskom balíku Office starú dva roky. Zariadenia, ktoré nemajú z nejakého dôvodu ešte aktualizácie tejto chyby CVE-2017-11882 v module Equation Editor, sú aktuálne ohrozené. Zraniteľnosť umožňuje útočníkom po otvorení škodlivého dokumentu vzdialene vykonávať kód bez ďalšej interakcie obete. Útočníci začali rozosielať nevyžiadané emaily, ktoré obsahovali infikovaný dokument RTF. Po otvorení takto infikovaného dokumentu sa stiahol trójsky kôň a v počítači vytvoril zadné vrátka. Záplata na túto zraniteľnosť existuje už od roku 2017. Viac informácií na stránke.

Nový phishingový útok cez email

Útok spočíva v prezentovaní používateľovi zoznam e-mailov. Tieto e-maily majú čakať na doručenie a od používateľa sa očakáva, aby sa rozhodol, čo chce s danými e-mailmi spraviť. Môže ich odstrániť, odmietnuť alebo povoliť. Na ktorúkoľvek možnosť používateľ klikne, je presmerovaný na falošnú aplikáciu Outlook Web App, kde sa zobrazí výzva, aby zadal svoje prihlasovacie údaje. Všetky údaje sa ukladajú na serveri útočníka, ktorý ich môže neskôr zneužiť. Viac informácií na stránke.

Útočníci dokážu obísť bezpečnostnú kontrolu v macOS Mojave

Operačný systém spoločnosti Apple, MacOS Mojave, obsahuje zraniteľnosti, ktoré umožňujú prostredníctvom malvéru vykonávať syntetické kliknutia a obchádzať tak bezpečnostné prvky systému. Útočník tak môže získať prístup k citlivým údajom pre aplikácie, ktoré si na to musia pýtať povolenie. Môže tiež nainštalovať zraniteľné rozšírenia jadra, ktoré môže zneužiť na ďalšiu fázu útoku a ovládnutie zariadenia. Viac informácií nájdete na našej stránke.

Závažné zraniteľnosti v Kace K1000

V zariadeniach Kace K1000 sa nachádza niekoľko závažných zraniteľností, ktoré umožňujú autentifikovanému útočníkovi prístup k citlivým údajom z aplikačnej databázy a vykonávať JavaScript kód. Zároveň môže vzdialene aj bez autentifikácie pridať nový administrátorský účet, alebo meniť nastavenia na zraniteľnom zariadení. Viac informácií nájdete na našej stránke.

Závažné zraniteľnosti rkt Container umožňujú root prístup k systému

Prostredie rkt Container obsahuje závažné zraniteľnosti, ktoré umožňujú kvôli nedostatočnej ochrane vzdialene vykonávať kód a uniknúť z kontajnera. Pri tom môže úspešný útočník získať root práva na hostiteľskom systéme. Opravné aktualizácie nie sú plánované. Viac informácií sa dozviete tu.

Zero-day zraniteľnosť RDP na Windows 10 umožňuje prístup ku vzdialenému systému

Novo objavená zero-day zraniteľnosť pripojenia RDP autentifikovaného pomocou NLA umožňuje lokálnemu útočníkovi po krátkom prerušení konektivity získať prístup ku vzdialenému systému. Relácia sa totiž obnoví v nezamknutom stave, aj ak obeť pred odchodom od klientskej stanice vzdialený systém zamkla. Nezáleží ani na tom, či systém využíva viacfaktorovú autentifikáciu, či inú dodatočnú ochranu. Pokračovanie na stránke.