Mesačný prehľad kritických zraniteľností
Máj 2019

1. Operačné systémy Microsoft Windows

Spoločnosť opravila v mesiaci máj 3 kritické zraniteľnosti.

Kritická zraniteľnosť CVE-2019-0708 v operačnom systéme Windows / Windows Server sa nachádza v službe Remote Desktop Services. Neautorizovanému útočníkovi umožňuje bez interakcie používateľa vzdialene vykonávať kód a prevziať plnú kontrolu nad zraniteľným zariadením. Obdobná zraniteľnosť umožnila v roku 2017 šírenie ransomvéru WannaCry. Viac na našej stránke.

Opravená bola aj zraniteľnosť CVE-2019-0903 v komponente Graphics Device Interface(GDI+). Táto zraniteľnosť vzniká pri pristupovaní komponentu ku objektom v pamäti 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.

Ďalšia kritická zraniteľnosť CVE-2019-0725 sa týka DHCP servera. Útočník môže poškodiť pamäť, ak pošle špeciálne upravené DHCP odpovede klientovi. Po zneužití dokáže vykonávať škodlivý kód na zariadení klienta.

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://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=251

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0903

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0725

2. Kancelárske balíky Microsoft Office a Office Web Apps

Tento mesiac bola opravená 1 kritická zraniteľnosť.

Zraniteľnosť vzdialeného vykonávania kódu CVE-2019-0953 je spôsobená tým, že Microsoft Word nesprávne pracuje s objektmi v pamäti. Na zneužitie môže útočník použiť špeciálne pripravený súbor. Potom musí ešte presvedčiť 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. Môže napríklad spustiť kód ako práve prihlásený používateľ.

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-2019-0953

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft opravila v mesiaci máj 4 kritické zraniteľnosti.

Zraniteľnosť CVE-2019-0884, CVE-2019-0918 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 cez Internet Explorer. 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.

CVE-2019-0940, CVE-2019-0929 zraniteľnosť vzniká pri pristupovaní prehliadačov ku objektom v pamäti. Na zneužitie zraniteľnosti útočník môže hostiť webstránku, ktorej obsah je prispôsobený na využitie tejto zraniteľnosti cez Interner 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-2019-0884

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0940

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0918

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0929

Microsoft Edge

Spoločnosť Microsoft opravila tento mesiac 12 kritických zraniteľností. Zraniteľnosť CVE-2019-0913 – CVE-2019-0917 a CVE-2019-0922, CVE-2019-0924 až CVE-2019-0927 (s výnimkou CVE-2019-0926), CVE-2019-0933 a CVE-2019-0937 umožňuje vzdialené vykonávanie kódu, ak Chakra skriptovací nástroj nevhodne pristupuje ku objektom v pamäti. Na zneužitie tejto zraniteľnosti je potrebné hostiť webstránku, ktorej obsah je prispôsobený na využitie danej zraniteľnosti cez Microsoft Edge. 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.

Zraniteľnosť CVE-2019-0926 vzniká, keď Microsoft Edge nevhodne pristupuje ku objektom v pamäti.

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-2019-0937
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0913
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0914
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0915
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0916
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0917
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0922
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0924
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0925
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0926
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0927
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0933

Mozilla Firefox

V mesiaci máj boli opravené 2 kritické zraniteľnosti.

CVE-2019-9814 a CVE-2019-9800 vznikajú pri poškodení pamäte a po zneužití dokážu útočníci vykonávať ľubovoľný kód.

Opravených bolo aj 13 závažných zraniteľností. Medzi nich patrí zraniteľnosť CVE-2019-7317 typu „use-after-free"(použitie odalokovaného miesta v pamäti), ktorá bola objavená v libpng knižnici vo funkcii png_image_free. Taktiež CVE-2019-11693, ktorá sa vyskytuje iba na operačných systémoch Linux. Je spôsobená pretečením vyrovnávacej pamäte. Ďalšie zraniteľnosti CVE-2019-11692, CVE-2019-11691, CVE-2019-9820 sú tiež typu „use-after-free".

Zdroje:

https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-14/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-13/

Google Chrome

V mesiaci máj nebola opravená žiadna kritická zraniteľnosť. Opravené boli iba zraniteľnosti nízkej závažnosti.

Zraniteľné systémy:

Google Chrome verzie staršie ako 74.0.3729.159

Odporúčania:

Odporúčame aktualizáciu na novšiu verziu 74.0.3729.159.

Zdroje:

https://chromereleases.googleblog.com/2019
https://chromereleases.googleblog.com/2019/05/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2019/05/stable-channel-update-for-chrome-os_17.html

4. Adobe Flash Player, Acrobat a Reader

Adobe Flash Acrobat a Reader

Adobe zverejnil update pre Adobe Acrobat a Reader na operačných systémoch Windows, ktorý slúži na zabezpečenie kritických a závažných zraniteľností. 36 kritických zraniteľností je

typu „use-after-free“ (používanie odalokovaného miesta v pamäti). Medzi nich patrí napríklad CVE-2019-7834, CVE-2019-7821, CVE-2019-7782, CVE-2019-7765 a CVE-2019-7759. Opravených bolo aj 6 kritických zraniteľností, ktoré vznikajú pri zapisovaní do pamäte mimo hraníc. Zraniteľnosť CVE-2019-7820 vzniká pri nezhode typov. Kritické zraniteľnosti CVE-2019-7828, CVE-2019-7827 sú spôsobené pretečením haldy. CVE-2019-7824 vzniká pri chybe vo vyrovnávacej pamäti, CVE-2019-7784 pri dvojnásobnom odalokovaní toho istého miesta v pamäti a CVE-2019-7779 pri obchádzaní určitých bezpečnostných obmedzení. Každá z týchto zraniteľností umožňuje vykonávať ľubovoľný kód.

Ďalších 35 zraniteľností je závažných. Sú spôsobené čítaním pamäte mimo hraníc a umožňujú únik používateľských informácií.

Zraniteľné systémy:

Acrobat DC 2019.010.20100 a staršie
Acrobat Reader DC 2019.010.20099 a staršie
Acrobat 2017 2017.011.30140 a staršie
Acrobat Reader 2017.011.30138 a staršie
Acrobat DC 2015.006.30495 a staršie
Acrobat Reader DC 2015.006.30493 a staršie

Adobe Flash Player

Pre Adobe Flash Player bola zverejnená aktualizácia opravujúca kritickú zraniteľnosť CVE-2019-7837. Táto zraniteľnosť bola typu „use-after-free“, (používanie odalokovaného miesta v pamäti) a umožňuje vykonávať útočníkom ľubovoľný kód.

Zraniteľné systémy:

Adobe Flash Player Desktop Runtime 32.0.0.171 a staršie
Adobe Flash Player for Google Chrome 32.0.0.171 a staršie
Adobe Flash Player for Microsoft Edge and Internet Explorer 11 32.0.0.171 a staršie

Odporúčania:

Vzhľadom na veľký počet kritických zraniteľností odporúčame používateľom aktualizovať softvér na najnovšiu verziu.

Zdroje:

https://helpx.adobe.com/security.html
https://helpx.adobe.com/security/products/flash-player/apsb19-26.html
https://helpx.adobe.com/security/products/acrobat/apsb19-18.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

Windows 10 zero-day zraniteľnosť od SandboxEscapera

Výskumník s pseudonymom SandboxEscaper zverejnil ďalší ukážkový kód na zneužitie zero-day zraniteľnosti v systéme Windows 10. Zraniteľnosť sa nachádza v nástroji Task Scheduler a dovoľuje útočníkom zvýšiť práva až na úroveň systému. Následne je možné vykonávať ľubovoľný kód s právami systému. Na zraniteľnosť zatiaľ neexistuje opravná aktualizácia. Viac informácií tu.

Nové zraniteľnosti procesorov Intel

Bezpečnostní výskumníci objavili viacero zraniteľností procesorov Intel. Milióny počítačov sú v ohrození. Zraniteľnosti umožňujú čítať citlivé údaje vrátane hesiel, tokenov a histórie webových prehliadačov, zneužitím bočného kanála pri vykonávaní špekulatívnej exekúcie. Aplikácia opráv spôsobí zníženie výkonu procesorov, ktorého veľkosť záleží od ich konkrétnej aplikácie. Najviac zasiahnuté budú pravdepodobne dátové centrá. Vzhľadom na povahu zraniteľností sa predpokladá cielené zneužívanie, nie plošná kampaň. Ďalšie informácie si môžete prečítať na našej stránke.

Zraniteľnosti v PrintLogic dovoľujú útočníkom meniť konfiguračné súbory a vzdialene vykonávať kód

V softvéri PrintLogic Management boli objavené tri zraniteľnosti umožňujúce vzdialene vykonávať ľubovoľný kód a upravovať konfiguračné súbory programu. Útočníci to môžu dosiahnuť predstieraním cudzej identity, DNS spoofingom, modifikovaním sťahovaného kódu, či vkladaním špeciálnych znakov do webového prehliadača, z ktorého vstupy program nekontroluje. Viac informácií na stránke.

Kritická zraniteľnosť v Linux Kernel

V implementácii protokolu TCP/IP linuxového jadra sa nachádza zraniteľnosť, ktorá použitím odalokovanej pamäte umožňuje vzdialene vykonávať na zraniteľnom zariadení ľubovoľný kód. Viac informácií na stránke.

Kaspersky - zraniteľné sú aj antivírusy

Bezpečnostní výskumníci z tímu Imaginary objavili zraniteľnosť, ktorá sa vyskytuje v antivírovom programe spoločnosti Kaspersky Lab a umožňuje vykonávanie ľubovoľného kódu v kontexte aplikácie. Viac informácií na stránke.

Kritická zraniteľnosť Windows - zneužiteľné RDP na voľné šírenie malvéru

Kritická zraniteľnosť v operačnom systéme Windows / Windows Server sa nachádza v službe Remote Desktop Services. Neautorizovanému útočníkovi umožňuje bez interakcie používateľa vzdialene vykonávať kód a prevziať plnú kontrolu nad zraniteľným zariadením. Obdobná zraniteľnosť umožnila v roku 2017 šírenie ransomvéru WannaCry. Viac informácií na stránke.

Varovanie pre organizácie používajúce SAP aplikácie

Až 90% inštancií SAP systému vo svete používa nesprávnu konfiguráciu prístupových pravidiel umožňujúcu útočníkom registrovať ľubovoľné nové aplikačné servery. To môže viesť až ku prevzatiu

kontroly nad zraniteľnými systémami. Nakoľko minulý mesiac výskumníci zverejnili ukážkový kód na zneužitie tejto zraniteľnosti, počet útokov na zraniteľné systémy SAP stúpa. Viac informácií na stránke.

DELL - predinštalovaný nástroj SupportAssist umožňuje vzdialene vykonávať kód

Kritická zraniteľnosť v nástroji Dell SupportAssist, ktorý je predinštalovaný na väčšine Dell počítačov, umožňuje útočníkom nahrať a vzdialene vykonávať na zraniteľnom zariadení ľubovoľný kód. To môže viesť až ku prevzatiu kontroly nad zariadením. Nástroj sa preto odporúča bezodkladne aktualizovať, alebo odinštalovať. Viac informácií na stránke.

Nedôveryhodné podpisy v e-mailových klientoch

Zraniteľnosti pri overovaní e-mailových podpisov v implementáciách OpenPGP a S/MIME dovoľujú vo viacerých bežne používaných e-mailových klientoch útočníkom presvedčivo falšovať podpisy správ, a tak presvedčiť svoje obete, že prijaté správy pochádzajú od dôveryhodného zdroja. Bezpečností výskumníci kategorizovali päť druhov útokov na autentifikáciu e-mailov kryptografickým podpisom. Viac informácií na stránke.

Zraniteľnosť na serveri Apache Tomcat umožňuje prevziať kontrolu nad zariadením

Na serveri Apache Tomcat v servlete Common Gateway Interface bola nájdená zraniteľnosť, ktorá umožňuje vzdialené vykonávanie kódu. Zraniteľnosť súvisí so spôsobom, akým Java Runtime Environment (JRE) odovzdáva argumenty pre príkazový riadok operačného systému Windows. Útočník môže ovládnuť Windows server, na ktorom beží zraniteľná verzia Apache Tomcat. Viac informácií na stránke.