Mesačný prehľad kritických zraniteľností
marec 2020

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci marec 8 kritických a 71 závažných zraniteľností.

Opravená bola kritická zraniteľnosť CVE-2020-0684, ktorá môže umožniť vzdialené vykonanie kódu pri spracovávaní súboru s príponou .LNK. Útočník môže zneužitím tejto zraniteľnosti získať rovnaké používateľské práva ako lokálny používateľ.

Ďalšou opravenou zraniteľnosťou je CVE-2020-0796, vznikajúca spôsobom akým protokol Microsoft Server Message Block 3.1.1 (SMBv3) spracováva určité požiadavky. Útočník, ktorý by túto zraniteľnosť úspešne zneužil, by mohol získať schopnosť vzdialene vykonať kód na cieľovom serveri alebo klientovi.

Opravené boli kritické zraniteľnosti CVE-2020-0801, CVE-2020-0807, CVE-2020-0809 a CVE-2020-0869 nachádzajúce sa vo Windows Media Foundation, ktorý nesprávne spracúva objekty v pamäti. Po ich zneužití môže útočník inštalovať programy, prezerať, mazať a meniť dáta a vytvárať účty s plnými používateľskými právami.

Zraniteľnosti CVE-2020-0881 a CVE-2020-0883 vznikajú spôsobom akým rozhranie GDI (Windows Graphics Device Interface) spracováva objekty v pamäti. Po ich zneužití môže útočník inštalovať programy, prezerať, mazať a meniť dáta a vytvárať účty s plnými používateľskými právami.

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 1709 for 32-bit Systems
Windows 10 Version 1709 for ARM64-based Systems
Windows 10 Version 1709 for x64-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 10 Version 1909 for 32-bit Systems
Windows 10 Version 1909 for ARM64-based Systems
Windows 10 Version 1909 for x64-based Systems
Windows 8.1 for 32-bit systems
Windows 8.1 for x64-based systems
Windows RT 8.1
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 1803 (Server Core Installation)
Windows Server, version 1903 (Server Core installation)
Windows Server, version 1909 (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-2020-0684
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0796
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0801
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0807
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0809
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0869
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0881
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0883

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft opravila v mesiaci marec 1 závažnú zraniteľnosť.

Zraniteľnosť CVE-2020-0852 vzniká v spôsobe akým Microsoft Word spracováva objekty v pamäti. Útočník môže zneužitím tejto zraniteľnosti vykonávať akcie v kontexte aktuálneho používateľa, teda potenciálne aj s administrátorskými právami.

Zraniteľné systémy:
Microsoft Office 2016 for Mac
Microsoft Office 2019 for 32-bit editions
Microsoft Office 2019 for 64-bit editions
Microsoft Office Online Server
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-2020-0852

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft opravila tento mesiac v prehliadači Internet Explorer 6 kritických zraniteľností.

Zraniteľnosť CVE-2020-0786 vzniká kvôli nesprávnemu spracovávaniu odkazov službou Windows Tile Object Service. Zneužitie tejto chyby by útočníkovi mohlo umožniť prepísať systémové súbory alebo vykonať útok zahltením servera služby (DoS).

Internet Explorer neoprávnene pristupuje k objektom v pamäti, čo umožňuje využitie zraniteľnosti CVE-2020-0824. Táto chyba zabezpečenia by mohla poškodiť pamäť takým spôsobom, že by útočník mohol vzdialene vykonať ľubovoľný kód v kontexte aktuálneho používateľa.

Opravené boli zraniteľnosti CVE-2020-0830, CVE-2020-0832 a CVE-2020-0833, ktorých zneužitie umožňujú útočníkovi vykonávať kód v kontexte aktuálneho používateľa, teda potenciálne aj s administrátorskými právami. Útočník tak môže inštalovať programy, prezerať, mazať a meniť dáta a vytvárať účty s plnými používateľskými právami.

Zraniteľnosť CVE-2020-0847 rovnako ako predchádzajúce vzniká v dôsledku nesprávnemu spracovávaniu objektov v pamäti. Jej zneužitie umožňuje útočníkovi vykonávať kód v kontexte aktuálneho používateľa, teda potenciálne aj s administrátorskými právami. Útočník tak môže inštalovať programy, prezerať, mazať a meniť dáta a vytvárať účty s plnými používateľskými právami.

Zraniteľné systémy:
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-2020-0786
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0824
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0830
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0832
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0833
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0847

Microsoft Edge

Spoločnosť Microsoft opravila tento mesiac v prehliadači Microsoft Edge 13 kritických zraniteľností.

Opravené boli kritické zraniteľnosti CVE-2020-0768, CVE-2020-0811, CVE-2020-0812, CVE-2020-0816, CVE-2020-0823, CVE-2020-0825 - CVE-2020-0831 a CVE-2020-0848. Tieto zraniteľnosti vznikajú pri nesprávnom spracovávaní objektov v pamäti prehliadača. Ich zneužitie umožňuje útočníkovi vykonávať kód v kontexte aktuálneho používateľa, teda potenciálne aj s administrátorskými právami. Útočník tak môže inštalovať programy, prezerať, mazať a meniť dáta a vytvárať účty s plnými používateľskými právami.

Zraniteľné systémy:
Microsoft Edge (EdgeHTML-based) v systémoch Windows 10

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-2020-0768
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0811
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0812
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0816
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0823
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0825
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0826
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0827
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0828
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0829
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0830
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0831
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0848

Mozilla Firefox

V mesiaci marec boli opravené 3 závažné zraniteľnosti.

Závažná zraniteľnosť CVE-2020-6796 môže spôsobiť poškodenie pamäte modifikovaním zdieľanej pamäte súvisiacej s informáciami o hlásení zlyhania a samotnom zlyhaní. Zraniteľnosti CVE-2020-6800 a CVE-2020-6801 takisto súvisia s poškodením pamäte a môžu byť zneužité na vzdialené vykonávanie kódu útočníkom.

Zraniteľné systémy:
Mozilla Firefox verzie staršie ako 74
Mozilla Firefox ESR verzie staršie ako 68.6

Odporúčania:
Odporúčame aktualizáciu na verziu 74 resp. Firefox ESR 68.6.

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-08/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-09/

Google Chrome

V mesiaci marec bola vydaná oprava na 3 závažné zraniteľnosti.

Opravené boli závažné zraniteľnosti CVE-2020-6450 a CVE-2020-6451 týkajúce sa poškodenia pamäti v rozšírení Web Audio a zraniteľnosť CVE-2020-6452 týkajúca sa pretečenia medzipamäte haldy.

Zraniteľné systémy:
Google Chrome verzie staršie ako 80.0.3987.162

Odporúčania:
Odporúčame aktualizáciu na verziu 80.0.3987.162

Zdroje:
https://chromereleases.googleblog.com/2020
https://chromereleases.googleblog.com/2020/03/stable-channel-update-for-desktop_31.html

4. Adobe Flash Player, Acrobat a Reader

V mesiaci marec nevydala spoločnosť Adobe opravu žiadnej zraniteľnosti pre Adobe Flash Player. V Adobe Acrobat and Reader bolo opravených 9 kritických a 4 závažné zraniteľnosti.

Zneužitie kritických zraniteľností, ktoré boli opravené v Adobe Acrobat and Reader môže útočníkom umožniť okrem vzdialeného vykonávania kódu taktiež vyzradenie informácií, zvýšenie oprávnení či zápis do súborového systému. Zraniteľnosti sa týkajú poškodenia pamäte a pretečenia zásobníka medzipamäte.

Zraniteľné systémy:
Acrobat DC
Acrobat Reader DC
Acrobat 2017

Acrobat Reader 2017
Acrobat 2015
Acrobat Reader 2015

Odporúčania:
Odporúčame aktualizáciu:
Acrobat DC, Acrobat Reader DC na verziu 2020.006.20042
Acrobat 2017, Acrobat Reader 2017 na verziu 2017.011.30166
Acrobat 2015, Acrobat Reader 2015 na verziu 2015.006.30518

Zdroje:
https://helpx.adobe.com/security.html
https://helpx.adobe.com/security/products/acrobat/apsb20-13.html

5. Frameworky

Microsoft .NET Framework

V mesiaci marec nevydala spoločnosť Microsoft žiadne opravné aktualizácie pre .NET Framework.

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

Oracle Java

Veľká sada opráv je plánovaná na 14. apríla 2020.

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

6. Iné závažné zraniteľnosti

ZyXEL vydal opravu zero-day zraniteľnosti ovplyvňujúcej jeho NAS zariadenia

Zraniteľnosť CVE-2020-9054, ovplyvňuje množstvo NAS a firewall zariadení od spoločnosti ZyXEL. Umožňuje vzdialené vykonávanie kódu bez potreby interakcie na zariadení cez

vkladanie príkazov počas autentifikácie. Spoločnosť vydala aktualizácie, ale niektoré staršie zraniteľné zariadenia aktualizované nebudú. Na internete je dostupný exploit. Viac informácií na stránke.

Útočníci masovo hľadajú zraniteľné Microsoft Exchange servery

Závažná zraniteľnosť umožňujúca vzdialene vykonávať kód sa týka všetkých verzií Microsoft Exchange servera. Pri inštalácii zlyhá tvorba unikátnych kryptografických kľúčov a použijú sa statické kľúče ktoré majú všetky servery rovnaké, čo možno využiť po autentifikácii na spúšťanie príkazov a kódu so SYSTEM oprávnením v rámci komponentu Exchange Control Panel a manipuláciu s e-mailovými správami na serveri. Viac informácií na stránke.

OpenSMTPD má dve vážne zraniteľnosti, na obe je už záplata

Zraniteľnosti sa týkajú mail servera OpenSMTPD. Prvá je stredne závažná zraniteľnosť, ktorá umožňuje bez privilégií čítať prvý riadok súborov, alebo v istých prípadoch celé súbory používateľov. Druhá je kritická zraniteľnosť umožňujúca čítanie pamäte mimo povolených hodnôt. Pochádza ešte z roku 2015 a umožňuje vzdialenému útočníkovi vykonávať shell príkazy, ktoré vloží do SMTP obálky. Po aktualizácii z mája 2018 môže útočník vykonávať príkazy aj s právami root. Viac informácií na stránke.

Kr00k zraniteľnosť zasahuje až miliardu zariadení

Zraniteľnosť CVE-2019-15126 sa nachádza vo WiFi čipoch vyrobených spoločnosťami Broadcom a Cypress, používanými v koncových zariadeniach, routeroch a prístupových bodoch. Zraniteľnosť spôsobuje, že čip použije nulový dočasný kľúč na šifrovanie paketov, ktoré odošle po odpojení z WiFi siete. Dáta z týchto paketov môže útočník odchytiť a využiť pri ďalších útokoch. Viac informácií na stránke.

Kritická zraniteľnosť Ghostcat zasahuje Apache Tomcat

Zraniteľnosť CVE-2020-1938 ovplyvňuje Apache Tomcat vo verziách 6 až 9, vydaných za posledných 13 rokov. Umožňuje vzdialené čítanie súborov webových aplikácií na Tomcat serveri a pre webové aplikácie, ktoré umožňujú ukladanie súborov, je možné vložiť súbory s JSP kódom priamo do aplikácie. Pre verzie 7 až 9 je vydaná bezpečnostná aktualizácia, verzia 6 už nie je podporovaná. Útočníci už aktívne skenujú zraniteľné servery. Viac informácií na stránke.

PPPD má 17 rokov starú kritickú zraniteľnosť umožňujúcu vzdialene vykonávať kód

Implementácia Point-to-Point protokolu – PPPD v mnohých distribúciách systému Linux má zraniteľnosť pretečenia medzipamäte, ktorá umožňuje útočníkovi po poslaní deformovaného EAP paketu vzdialene vykonávať kód na serveri alebo klientovi. Útočník nemusí byť autentifikovaný a PPPD príjme aj nevyžiadané pakety. Útočníkov kód sa môže vykonať s root oprávneniami. Viac informácií na stránke.

Zero-day zraniteľnosť Zoho ManageEngine umožňuje vzdialené vykonávanie kódu

Služba Zoho ManageEngine Desktop Central, slúžiaca na manažment vzdialených zariadení, nesprávne kontroluje vstupné dáta od používateľa. Takto môže softvér deserializovať nedôveryhodné dáta, čo útočníkovi dáva možnosť vykonávať kód s oprávneniami SYSTEM alebo root bez potreby autentifikácie na zraniteľnom zaradení a prevziať kontrolu nad spravovanými zariadeniami. Viac informácií na stránke.

Kritická zraniteľnosť typu „wormable“ umožňuje vzdialené vykonávanie kódu v Microsoft Server Message Block 3.1.1.

Spoločnosť Microsoft zverejnila 10. marca upozornenie ADV200005, týkajúce sa kritickej zraniteľnosti zneužiteľnej na vzdialené vykonávanie kódu v protokole Microsoft Server Message Block 3.1.1 (SMBv3). Táto zraniteľnosť je spôsobená chybou spracúvania skomprimovaných škodlivých dátových paketov. Neautentifikovanému útočníkovi umožňuje zneužitie tejto chyby vykonávať ľubovoľný kód v kontexte aplikácie. Útok môže byť vedený na SMBv3 servery, aj klientov. Viac informácií na stránke.

Kritická zraniteľnosť v produktoch VMware umožňuje vykonávanie kódu z hosťovaného systému

V produktoch od spoločnosti VMware boli nájdené 3 zraniteľnosti. Prvé dve zraniteľnosti sa týkajú VMware Workstation a Fusion. Prvá zraniteľnosť súvisí s použitím odalokovaného miesta v pamäti a umožňuje z hosťovaného systému vykonávať kód v hostiteľskom systéme. Druhá umožňuje eskaláciu privilégií na hosťovaných systémoch Linux, ktoré používajú

virtuálnu tlač. Tretia zraniteľnosť zasahuje len hostiteľské systémy Windows a produkty VMware Workstation, Horizon Client a VMRC a umožňuje lokálnemu používateľovi vykonávať príkazy ako ktorýkoľvek používateľ. Všetky zraniteľnosti sú v najnovších verziách produktov zaplátané. Viac informácií na stránke.

Dve neopravené kritické zero-day RCE zraniteľnosti zasahujú všetky verzie systému Windows

Spoločnosť Microsoft vydala upozornenie týkajúce sa bezpečnosti používateľov operačného systému Windows. Upozorňuje na dve nové kritické zero-day zraniteľnosti, ktoré umožňujú útočníkovi vzdialenú kontrolu nad napadnutými zariadeniami. Obe zraniteľnosti sú obmedzene zneužívané pri cielených útokoch a ovplyvňujú všetky podporované verzie operačného systému Windows. Nachádzajú sa v knižnici na analýzu písiem Windows Adobe Type Manager Library, ktorá nesprávnym spôsobom spracúva špeciálne vytvorené písmo Adobe Type 1 PostScript. Viac informácií na stránke.