Mesačný prehľad kritických zraniteľností
Apríl 2020

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci apríl 9 kritických a 59 závažných zraniteľností.

Opravených bolo 6 kritických zraniteľností umožňujúcich vzdialené vykonávanie kódu. Zraniteľnosť CVE-2020-0907 sa vyskytuje spôsobe, akým súčasti Microsoft Graphics Components spracúvajú objekty v pamäti. Zraniteľnosť CVE-2020-0687 vzniká pri nesprávnom spracovaní špeciálne vytvorených fontov. Po jej zneužití môže útočník inštalovať programy, prezerať, mazať a meniť dáta.

Ďalšia kritická zraniteľnosť CVE-2020-0910 vzniká, pretože Windows Hyper-V na hostiteľskom serveri nedokáže správne overiť vstup autentifikovaného používateľa v hosťujúcom operačnom systéme. Ak by útočník zneužil túto zraniteľnosť, mohol by na hosťujúcom operačnom systéme spustiť špeciálne vytvorenú aplikáciu, ktorá by mohla spôsobiť, že operačný systém hostiteľa Hyper-V vykoná ľubovoľný kód.

Opravená kritická zraniteľnosť CVE-2020-0965 existuje v spôsobe, akým knižnica kódov Microsoft Windows Codecs spracováva objekty v pamäti a takisto umožňuje útočníkovi vzdialene vykonať ľubovoľný kód.

Opravené boli kritické zraniteľnosti CVE-2020-0938 a CVE-2020-1020, ktoré vznikajú keď knižnica Adobe Type Manager Library systému Windows nesprávne manipuluje so špeciálne vytvoreným multi-master fontom - Adobe Type 1 PostScript. Útočník, ktorý úspešne zneužil túto chybu zabezpečenia, by mohol vo všetkých systémoch okrem systému Windows 10 vykonať kód na diaľku. Po jej zneužití môže útočník inštalovať programy, prezerať, mazať a meniť dáta.

Kritické zraniteľnosti CVE-2020-0948, CVE-2020-0949 a CVE-2020-0950 vznikajú pri nesprávnom spracúvaní objektov v pamäti programom Windows Media Foundation. Po ich zneužití môže útočník inštalovať programy, prezerať, mazať a meniť dáta.

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-2020-0687
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0907
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0910
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0938
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0948
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0949

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0950
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0965
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1020

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft opravila v mesiaci apríl 4 kritické a 28 závažných zraniteľností.

Opravené boli kritické zraniteľnosti CVE-2020-0929, CVE-2020-0931, CVE-2020-0932 a CVE-2020-0974. Všetky tieto zraniteľnosti vznikajú v prípade, že softvér nedokáže skontrolovať zdrojové označenie balíka aplikácií programu Microsoft SharePoint. Útočník, ktorý úspešne zneužije túto chybu zabezpečenia, by mohol spustiť ľubovoľný kód v kontexte aplikácie SharePoint. Využitie tejto chyby zabezpečenia vyžaduje, aby používateľ vložil špeciálne vytvorený balík aplikácií SharePoint do postihnutej verzie.

Zraniteľné systémy:
Microsoft SharePoint Server 2019
Microsoft SharePoint Foundation 2013 Service Pack 1
Microsoft SharePoint Foundation 2010 Service Pack 2
Microsoft SharePoint Enterprise Server 2016

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-2020-0929
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0931
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0932
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0974

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft opravila tento mesiac v prehliadači Internet Explorer 2 kritické zraniteľnosti.

Opravená bola zraniteľnosť CVE-2020-0967 vznikajúca pri chybnom spracúvaní objektov v pamäti modulom VBScript. Kritická zraniteľnosť CVE-2020-0968 vzniká v spôsobe, akým skriptovací stroj spracováva objekty v pamäti v programe Internet Explorer. Tieto chyby zabezpečenia by mohli poškodiť pamäť takým spôsobom, že by útočník mohol spustiť ľubovoľný kód v kontexte aktuálneho používateľa. Útočník môže po úspešnom zneužití týchto chýb zabezpečenia získať rovnaké používateľské práva ako súčasný používateľ. Po ich zneužití môže útočník inštalovať programy, prezerať, mazať a meniť dáta.

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-2020-0967
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0968

Microsoft Edge

Spoločnosť Microsoft opravila tento mesiac v prehliadači Microsoft Edge 2 kritické zraniteľnosti.

Zraniteľnosť CVE-2020-0969 vzniká v spôsobe akým skriptovací nástroj Chakra spracúva objekty v pamäti v aplikácii Microsoft Edge (založené na HTML). Táto chyba zabezpečenia by mohla poškodiť pamäť takým spôsobom, že by útočník mohol vykonať ľubovoľný kód v kontexte aktuálneho používateľa. Útočník, ktorý úspešne zneužil túto chybu zabezpečenia, by mohol získať rovnaké používateľské práva ako súčasný používateľ.

Kritická zraniteľnosť CVE-2020-0970 vzniká pri nesprávnom spracúvaní objektov v pamäti skriptovacím nástrojom ChakraCore. Útočník, ktorý úspešne zneužil túto chybu, by mohol získať rovnaké používateľské práva ako súčasný používateľ.

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-2020-0969
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0970

Mozilla Firefox

V mesiaci apríl boli opravené 2 kritické zraniteľnosti.

Obe opravené kritické zraniteľnosti sú typu "Use after free" (použitie odalokovaného miesta v pamäti). Zraniteľnosť CVE-2020-6819 môže za určitých podmienok spôsobiť spustenie deštruktora nsDocShell. Kritickú zraniteľnosť CVE-2020-6820 môže spôsobiť manipulácia s ReadableStream.

Zraniteľné systémy:
Mozilla Firefox verzie staršie ako 74.0.1
Mozilla Firefox ESR verzie staršie ako 68.6.1

Odporúčania:
Odporúčame aktualizáciu na verziu 74.0.1 resp. Firefox ESR 68.6.1.

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-11/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-12/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-13/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-14/

Google Chrome

V mesiaci február bola vydaná oprava na 2 závažné zraniteľnosti.

Závažná zraniteľnosť CVE-2020-6462 súvisí s použitím odalokovaného miesta v pamäti pri plánovaní úloh a zraniteľnosť CVE-2020-6461 súvisí s použitím odalokovaného miesta v pamäti úložiska.

Zraniteľné systémy:
Google Chrome verzie staršie ako 81.0.4044.129

Odporúčania:
Odporúčame aktualizáciu na verziu 81.0.4044.129

Zdroje:
https://chromereleases.googleblog.com/2020
https://chromereleases.googleblog.com/2020/04/stable-channel-update-for-desktop_27.html

4. Adobe Flash Player, Acrobat a Reader

V mesiaci apríl nevydala spoločnosť Adobe opravu žiadnych kritických zraniteľností pre Adobe Flash Player. V Adobe Acrobat a Reader bolo opravených 9 kritických a 4 závažných zraniteľností.

Zneužitie kritických zraniteľností, ktoré boli opravené v Adobe Acrobat a Reader môže útočníkom umožniť okrem vzdialeného vykonávania kódu taktiež vyzradenie informácií.

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 apríl nevydala spoločnosť Microsoft žiadne opravné aktualizácie pre .NET Framework.

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

Oracle Java

Spoločnosť Oracle vydala v mesiaci apríl plánovanú štvrťročnú veľkú sadu aktualizácií. V produkte Java SE a Java SE Embedded bolo celkovo opravených 15 zraniteľností. Prvé štyri najzávažnejšie CVE-2020-2803, CVE-2020-2805, CVE-2020-18197 a CVE-2020-2816 sa nachádzajú v knižniciach, a komponentoch JavaFX a JSSE.

Zraniteľné systémy:

Java SE: 7u251, 8u241, 11.0.6, 14
Java SE Embedded: 8u241

Odporúčania:

Odporúčame aktualizovať zraniteľné verzie Java SE a Java SE Embedded na aktuálne verzie, prostredníctvom Java Auto Update alebo na stránke spoločnosti Oracle, viď prvý odkaz v zdrojoch.

Zdroje:
https://www.oracle.com/technetwork/topics/security/alerts-086861.html
https://www.oracle.com/security-alerts/cpuapr2020.html#AppendixJAVA

6. Iné závažné zraniteľnosti

Zero-day zraniteľnosť aplikácie Zoom pre Windows umožňuje šírenie malvéru a vykonávanie kódu

V aplikácii Zoom zameriavajúcej sa na video konferenčné hovory bola nájdená kritická zero-day zraniteľnosť. Nachádza sa v klientovi aplikácie na operačnom systéme Windows. Táto zraniteľnosť vzniká v spôsobe akým aplikácia spracováva Uniform Resource Identifier (URI) cesty a jej zneužitie umožňuje útočníkovi vzdialené vykonávanie kódu. Po zneužití zraniteľnosti môže útočník získať informácie o sieti alebo tiež vykonať útok UNC injection (Universal Naming Convention). Viac informácií na stránke.

Cisco opravilo kritické zraniteľnosti vo viacerých produktoch

Spoločnosť Cisco vydala bezpečnostné záplaty na kritické a závažné zraniteľnosti viacerých produktov. Vzdialený útočník mohol tieto zraniteľnosti využiť so zámerom získať kontrolu nad postihnutým systémom, vykonávať kód, či spôsobiť nedostupnosť služby. Americká vládna agentúra CISA nabáda užívateľov a administrátorov, aby zraniteľné systémy bezodkladne aktualizovali. Viac informácií na stránke.

Závažné zraniteľnosti produktov Intel

Spoločnosť Intel opravila vo viacerých svojich produktoch deväť závažných a stredne závažných zraniteľností. Tieto umožňujú autentifikovaným aj neautentifikovaným útočníkom zvýšenie oprávnení a spôsobenie nedostupnosti služieb. Spoločnosť odporúča bezodkladnú aktualizáciu zraniteľných produktov. Viac informácií na stránke.

VMWare opravil kritickú zraniteľnosť vo vCenter Server a dve závažné vo vRealize Log Insight

Spoločnosť VMWare opravila kritickú zraniteľnosť v produkte vCenter Server, ktorá umožňovala útočníkom získať citlivé informácie zo služby Directory Service, s ktorých pomocou mohli prevziať kontrolu nad celou infraštruktúrou. Opravené boli aj dve zraniteľnosti v produkte vRealize Log Insight, ktoré kvôli nevhodnej kontrole vstupov umožňovali ovládnutie zraniteľných zariadení. Viac informácií na stránke.

Na platforme Git bola odstránená kritická zraniteľnosť

Vytvorením špeciálne upravenej adresy URL, ktorá obsahuje zakódovaný nový riadok, môžu byť do toku paketov vložené neočakávané hodnoty. Útočník tak môže pomocou špeciálne vytvorenej adresy URL docieliť, že klient Git vloží prihlasovacie údaje svojho hostiteľského serveru do HTTP požiadavky pre ľubovoľný cudzí server. Viac informácií na stránke.

Štyri zero-day zraniteľnosti produktu IBM Data Risk Manager boli zverejnené online

Na portáli Github boli zverejnené štyri kritické zraniteľnosti produktu IBM Data Risk Manager v kategóriách obídenie autentifikácie, vkladanie príkazov, nezabezpečené predvolené heslo a ľubovoľné sťahovanie súborov. Útočník ich zneužitím môže vzdialene vykonávať kód, sťahovať zo systému ľubovoľné súbory či ovládnuť zraniteľnú infraštruktúru. Viac informácií na stránke.

V knižnici Autodesk FBX boli opravené závažné zraniteľnosti

Spoločnosť Autodesk zverejnila opravy na bezpečnostné chyby nájdené v knižnici Autodesk FBX-SDK, ktorú využíva viacero systémov pre spracovanie 3D obsahu. Úspešné zneužitie zraniteľnosti umožňuje získanie kontroly nad cieľovým zariadením, vzdialené vykonanie ľubovoľného kódu alebo odmietnutie služby (DoS). Viac informácií na stránke.

Chyba OpenSSL umožňuje spôsobiť nedostupnosť služby

Nesprávne narábanie s rozšírením TLS 1.3 „signature_algorithms_cert“ vedie pri nadväzovaní spojenia medzi serverom a klientom a volaní funkcie SSL_check_chain() ku zlyhaniu aplikácie, čo má za následok vyvolanie nedostupnosti služby. Viac informácií na stránke.

Obídenie autentifikácie vo FortiMail a FortiVoiceEnterprise

Zraniteľnosť vo FortiMail a FortiVoiceEnterprise s označením CVE-2020-9294 umožňuje vzdialenému útočníkovi obídenie autentifikácie a získanie prístupu do systému ako oprávnený užívateľ. Viac informácií na stránke.

Foxit Reader, PhantomPDF a doplnok U3DBrowser obsahujú závažné bezpečnostné zraniteľnosti

Spoločnosť Foxit Software vydala záplaty závažných bezpečnostných zraniteľností pre jej platformy na čítanie a editáciu PDF. Niektoré z chýb umožňujú vzdialenému útočníkovi vykonať v zraniteľných systémoch ľubovoľný kód. Viac informácií na stránke.