Mesačný prehľad kritických zraniteľností
Máj 2020

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci Máj 5 kritických a 73 závažných zraniteľností.

Opravených bolo 5 kritických zraniteľností umožňujúcich vzdialené vykonávanie kódu. Zraniteľnosť CVE-2020-1153 súvisí so spôsobom, akým súčasti Microsoft Graphics Components spracúvajú objekty v pamäti. Zraniteľnosť CVE-2020-1136, CVE-2020-1126 a CVE-2020-1028 vzniká pri nesprávnom spracovaní špeciálne vytvorených fontov. Po jej zneužití môže útočník inštalovať programy, prezerať, mazať a meniť dáta.

Posledná opravená kritická zraniteľnosť CVE-2020-1117 bola objavená v spôsobe, akým modul správy farieb (ICM32.dll) spracováva objekty v pamäti. Útočník by mohol po jej zneužití prevziať kontrolu nad postihnutým systémom.

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-2020-1153
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1136
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1126
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1117
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1028

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft opravila v mesiaci máj 4 kritické a 9 závažných zraniteľností.

Opravené boli kritické zraniteľnosti CVE-2020-1023, CVE-2020-1024 a CVE-2020-1102 ktoré vznikajú v prípade, že softvér nedokáže skontrolovať zdrojové označenie balíka aplikácií programu Microsoft SharePoint. Útočník, ktorý úspešne zneužije túto chybu zabezpečenia, by mohol vykonávať ľubovoľný kód v kontexte aplikácie SharePoint. Využitie tejto chyby zabezpečenia vyžaduje, aby používateľ vložil špeciálne vytvorený balík aplikácií SharePoint do postihnutej verzie.

Opravená bola taktiež chyba CVE-2020-1069, ktorá sa týka Microsoft SharePoint Serveru. Server Microsoft SharePoint nedokáže správne identifikovať a filtrovať nebezpečné webové ovládacie prvky ASP.Net. Zneužitie tejto chyby by mohlo viesť k vykonaniu ľubovoľného kódu.

Aby útočník zneužil túto chybu zabezpečenia, musí autentifikovaný používateľ vytvoriť a vyvolať špeciálne vytvorenú stránku na zraniteľnej verzii Microsoft SharePoint Server.

Zraniteľné systémy:
Microsoft SharePoint Server 2019
Microsoft SharePoint Foundation 2013 Service Pack 1
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-2020-1023
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1024
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1069
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1102

3. Internetové prehliadače

Microsoft Internet Explorer

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

Opravená bola zraniteľnosť CVE-2020-1093 vznikajúca pri chybnom spracúvaní objektov v pamäti modulom VBScript. Kritická zraniteľnosť CVE-2020-1064 vzniká nesprávnym overovaním vstupov modulu MSHTML. Útočník by mohol vykonať ľubovoľný kód v kontexte aktuálneho používateľa. Ak je aktuálny používateľ prihlásený s právami administrátora, útočník, ktorý úspešne zneužil túto chybu, by mohol prevziať kontrolu nad postihnutým systémom. Útočník by potom mohol inštalovať programy, prezerať, meniť alebo mazať údaje.

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-2020-1093
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1064

Microsoft Edge

Spoločnosť Microsoft opravila tento mesiac v prehliadači Microsoft Edge 3 kritické zraniteľnosti.

Zraniteľnosť CVE-2020-1037 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-2020-1065 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.

Kritická zraniteľnosť CVE-2020-1065 je spôsobená nevynucovaním si pravidiel domén. Útočník by túto chybu mohol zneužiť na prístup k informáciám z jednej domény a vložiť ich do inej domény. Útočník, ktorý by úspešne zneužil túto chybu zabezpečenia by si mohol zvýšiť oprávnenia v postihnutých verziách programu Microsoft Edge.

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-2020-1037

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1056

Mozilla Firefox

V mesiaci máj boli opravené 3 kritické zraniteľnosti.

Prvá opravená kritická zraniteľnosť je typu "Use after free" (použitie odalokovaného miesta v pamäti). Zraniteľnosť CVE-2020-12387 môže za určitých podmienok spôsobiť spustenie deštruktora nsDocShell. Druhá kritická zraniteľnosť týkajúca sa Prehliadača Firefox v operačnom systéme Windows bola objavená a opravená v súčasti Sandbox, kde prehliadač dostatočne neblokuje riadenie prístupu a obsah odoslaný do tejto karantény z nej môže uniknúť.
Kritická zraniteľnosť bola objavená aj v emailovom klientovi Thunderbird. Zraniteľnosť je typu "Use after free", ktorá rovnako ako pri prehliadači Mozilla Firefox môže spôsobiť pád systému.

Zraniteľné systémy:
Mozilla Firefox verzie staršie ako 74.0.1
Mozilla Firefox ESR verzie staršie ako 68.6.1
Thunderbird verzie staršie ako 68.8

Odporúčania:
Odporúčame aktualizáciu na verziu 74.0.1 resp. Firefox ESR 68.6.1, v prípade Thunderbird na verziu 68.8

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-16/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-17/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-18/

Google Chrome

V mesiaci máj boli vydané opravy 7 závažných zraniteľností.

Závažná zraniteľnosť CVE-2020-6831 súvisí s pretečením vyrovnávacej pamäte pri analýze a overovaní blokov SCTP vo WebRTC. Zraniteľnosť CVE-2020-6464 súvisí s neoverovaním typu premennej v nástroji Blink a potencionálne je možné zneužiť ju cez podvrhnutú web stránku v jazyku HTML.

Opravené boli aj zraniteľnosti CVE-2020-6465, CVE-2020-6466 a CVE-2020-6467 súvisiace s použitím odalokovaného miesta v pamäti, zraniteľnosť CVE-2020-6468 v komponente V8 súvisiaca s neoverovaním typu premennej a zraniteľnosť CVE-2020-6469 súvisiaca s nedostatočne vyžadovanými politikami vo vývojárskych nástrojoch.

Zraniteľné systémy:
Google Chrome verzie staršie ako 81.0.4044.138

Odporúčania:
Odporúčame aktualizáciu na verziu 81.0.4044.138

Zdroje:
https://chromereleases.googleblog.com/2020
https://chromereleases.googleblog.com/2020/05/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2020/05/stable-channel-update-for-desktop_19.html

4. Adobe Flash Player, Acrobat a Reader

V mesiaci máj vydala spoločnosť Adobe opravu 6 kritických a 4 závažných zraniteľností pre Adobe Acrobat. Pre Adobe Flash Player a Adobe Reader neboli vydané záplaty.

Zneužitie kritických zraniteľností, ktoré boli opravené v Adobe Acrobat môže útočníkom umožniť vzdialené vykonanie kódu, pád aplikácie, obídenie zabezpečenia alebo získavanie 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/apsb20-24.html

5. Frameworky

Microsoft .NET Framework

V mesiaci máj vydala spoločnosť Microsoft opravné aktualizácie dvoch závažných zraniteľností pre .NET Framework.

Zraniteľnosť CVE-2020-1066 umožňuje útočníkom zvýšenie oprávnení. Na to je potrebné získať prístup do lokálneho zariadenia a spustiť škodlivý program. Zraniteľnosť CVE-2020-1108 súvisí s nevhodným narábaním webových požiadaviek a jej zneužitie môže viesť ku spôsobeniu nedostupnosti služby .NET Framework webovej aplikácie. Toto dokáže vzdialený neautentifikovaný útočník.

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-2020-1066
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1108

Oracle Java

Spoločnosť Oracle nevydala v mesiaci máj žiadne opravné aktualizácie pre svoje produkty.

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

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.

Spoločnosť Juniper vydala bezpečnostné aktualizácie pre Junos OS

Spoločnosť Juniper vydala bezpečnostné aktualizácie na opravu zraniteľnosti, ktorá ovplyvňovala viaceré verzie operačného systému Junos. Túto chybu mohol útočník zneužiť na prevzatie kontroly nad zraniteľným systémom. Útočníkom to tiež umožňovalo vzdialene vykonávať kód, obísť bezpečnostné obmedzenia a prístup k citlivým informáciám zo systému. Táto zraniteľnosť sa týka iba zariadení s OS Junos s povolenými službami HTTP/HTTPS. Viac informácií na stránke.

Protokol Samba – bezpečnostné aktualizácie pre viaceré verzie

Tím Samba vydal bezpečnostné aktualizácie opravujúce 2 zraniteľnosti týkajúce sa protokolu LDAP. Zneužitie týchto zraniteľností môže umožniť prístup ku odalokovanému miestu v pamäti a tiež narušenie dostupnosti systému. Na opravu týchto zraniteľností boli vydané nové verzie Samba 4.10.15, 4.11.8 a 4.12.2. Viac informácií na stránke.

Bezpečnostná chyba v MS Teams umožňuje prevzatie kontroly nad účtom

Bezpečnostná zraniteľnosť, nájdená v spôsobe načítania obrázkov GIF a overenia doručenia tohto typu súboru, umožňuje prebrať plnú kontrolu nad napadnutým účtom. Dochádza k tomu prostredníctvom obídenia autentifikácie API rozhrania MS Teams použitím dvoch získaných autentifikačných tokenov. Zraniteľnosť môže byť zneužitá v desktopovej aj webovej verzii aplikácie. Viac informácií na stránke.

Spoločnosť Cisco odstránila závažnú zraniteľnosť na IOS XE SD-WAN Software

Spoločnosť Cisco vydala bezpečnostnú záplatu na zraniteľnosť v Command Line Interface (CLI) systému Cisco IOS XE SD-WAN. Zraniteľnosť umožňuje overenému lokálnemu útočníkovi vykonať injekciu ľubovoľného príkazu, ktorý je realizovaný s právami ROOT. Bezpečnostná chyba je spôsobená nedostatočným overovaním príkazov na vstupe. Útočník môže zneužiť túto zraniteľnosť tak, že sa autentifikuje voči zariadeniu a vloží špeciálne upravený obsah do Command Line Interface CLI. Viac informácií na stránke.

Spoločnosť VMware vydala bezpečnostnú opravu XSS zraniteľnosti

Spoločnosť VMware vydala bezpečnostnú opravu zraniteľnosti XSS (cross-site scripting) s vysokou závažnosťou v produkte VMware ESXi. Zraniteľnosť CVE-2020-3955 bola popísaná v bezpečnostnom odporúčaní VMSA-2020-0008 vydanom na oficiálnej stránke VMware. Ovplyvňuje verzie VMware ESXi 6.5 a 6.7. Zverejnená zraniteľnosť umožňuje útočníkovi vzdialene vykonať HTML kód alebo skript na zraniteľnej webstránke. Viac informácií na stránke.

Spoločnosť SaltStack opravila kritické zraniteľnosti v softvéri Salt

Spoločnosť SaltStack vydala aktualizáciu, ktorá sa zameriava na opravu kritických zraniteľností ovplyvňujúcich verzie Salt staršie ako 2019.2.4 a 3000.2. Vzdialený útočník by tieto zraniteľnosti mohol zneužiť okrem iného na prevzatie kontroly nad postihnutým systémom. Niekoľko dní po vydaní varovaní sa útočníkom podarilo zneužiť tieto zraniteľnosti a napadnúť dve organizácie využívajúce technológiu SaltStack. Viac informácií na stránke.

Kritická zero-click zraniteľnosť Samsungu v szstéme Android verzie 8,9 a 10

V OS Android používanom spoločnosťou Samsung bola objavená kritická bezpečnostná chyba súvisiaca so spracovaním obrázkového formátu Qmage, ktorá umožňuje úplnú kompromitáciu

zariadenia pomocou MMS správ. Jej zneužitie nevyžaduje od obete žiadnu interakciu. Viac informácií na stránke.

BIAS – kritická zraniteľnosť v protokole Bluetooth

Vo všetkých zariadeniach využívajúcich protokol Bluetooth BR/EDR sa nachádza bezpečnostná zraniteľnosť, ktorá umožňuje krádež identity už spárovaného zariadenia. Útočník sa môže bez ďalšieho overovania pripojiť na hostiteľské zariadenie. Viac informácií na stránke.

Päť zero-day zraniteľností vo Windows umožňuje získať vyššie práva

Bezpečnostní experti spoločnosti Trend Micro Zero Day Initiative (ZDI) zverejnili informácie o piatich zneužívaných zraniteľnostiach operačného systému Windows, na ktoré zatiaľ neexistujú záplaty. Útočník by ich mohol zneužiť pre získanie vyšších používateľských oprávnení na postihnutom systéme. Tieto bezpečnostné chyby boli identifikované v hostiteľskom procese splwow64.exe pre tlačiarenské ovládače a sú spôsobené nesprávnym overovaním vstupných hodnôt zadávaných používateľom. Viac informácií na stránke.

Zraniteľnosť open-source webového redakčného systému Drupal

V redakčnom systéme Drupal core boli nájdené 2 závažné zraniteľnosti. Jednou je zraniteľnosť typu XSS, ktorá súvisí s dvomi zraniteľnosťami v Javascript knižnici jQuery, druhou zraniteľnosť typu Open redirect v Drupal 7. , ktoré umožňujú podvrhnúť súčasti stránky, alebo samotnú web stránku. Viac informácií na stránke.