Mesačný prehľad kritických zraniteľností
január 2020

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci január 3 kritické a 33 závažných zraniteľností.

Opravené boli kritické zraniteľnosti CVE-2020-0609 a CVE-2020-0610, ktoré umožňujú útočníkom vzdialene vykonávať kód. Nachádzajú sa vo Windows Remote Desktop Gateway. Neautentifikovaný útočník môže zneužiť tieto zraniteľnosti po pripojení na zraniteľný systém cez RDP odoslaním špeciálne vytvorených požiadaviek. Následne môže inštalovať programy, prezerať, mazať a meniť dáta a vytvárať účty s plnými používateľskými právami.

Kritická zraniteľnosť CVE-2020-0611 tiež umožňuje vzdialene vykonávať kód. Nachádza sa vo Windows Remote Desktop Client. Útočník môže zraniteľnosť zneužiť po tom, ako presvedčí obeť, aby sa pripojila na škodlivý server. Následne môže 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 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 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 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-2020-0609
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0610
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0611

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť opravila v mesiaci január 6 závažných zraniteľností.

Štyri opravené zraniteľnosti CVE-2020-0650 – CVE-2020-0653 umožňujú útočníkovi vzdialene vykonávať kód kvôli nevhodnému narábaniu s objektmi v pamäti. Útočník získa práva ako práve prihlásený používateľ a môže inštalovať programy, zobrazovať, meniť a mazať dáta a vytvárať nové používateľské účty. Pre zneužitie zraniteľnosti musí obeť otvoriť špeciálne vytvorený súbor.

Zraniteľnosť CVE-2020-0654 umožňuje útočníkovi obísť zabezpečenie aplikácie a CVE-2020-0647 umožňuje predstierať identitu obete kvôli nesprávnemu vyhodnocovaniu pôvodu.

Zraniteľné systémy:

Microsoft Office 2010 Service Pack 2 (32-bit editions)
Microsoft Office 2010 Service Pack 2 (64-bit editions)
Microsoft Office 2013 RT Service Pack 1
Microsoft Office 2013 Service Pack 1 (32-bit editions)
Microsoft Office 2013 Service Pack 1 (64-bit editions)
Microsoft Office 2016 (32-bit edition)
Microsoft Office 2016 (64-bit edition)

Microsoft Office 2016 for Mac
Microsoft Office 2019 for 32-bit editions
Microsoft Office 2019 for 64-bit editions
Microsoft Office 2019 for Mac
Office 365 ProPlus for 32-bit Systems
Office 365 ProPlus for 64-bit Systems
One Drive for Android
Office Online Server

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-2020-0647
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0650
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0651
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0652
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0653
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0654

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft opravila tento mesiac v prehliadači Internet Explorer 1 kritickú zraniteľnosť.

Zraniteľnosť CVE-2020-0640 umožňuje útočníkom vzdialene vykonávať kód kvôli nevhodnému prístupu k objektom v pamäti. Útočník získa práva ako práve prihlásený používateľ a môže inštalovať programy, zobrazovať, meniť a mazať dáta a vytvárať nové používateľské účty. Pre zneužitie zraniteľnosti musí presvedčiť obeť, aby navštívila špeciálne vytvorenú škodlivú webstránku.

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-2020-0640

Microsoft Edge
Spoločnosť Microsoft v mesiaci január neopravila v prehliadači Edge žiadnu kritických, ani závažnú zraniteľností.

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

Mozilla Firefox
V mesiaci január bolo opravených 1 kritická a 5 závažných zraniteľností.

Kritická zraniteľnosť CVE-2020-17026 sa nachádza v komponente IonMonkey JIT, kedy pri vytváraní polí môže nesprávny alias viesť k neovereniu typu premennej. Táto zraniteľnosť je reálne zneužívaná.

Závažná zraniteľnosť CVE-2020-17015 súvisí s poškodením pamäte v rodičovskom procese pri inicializácii nového obsahového procesu vo OS Windows. Zraniteľnosť CVE-2020-17016 umožňuje únik dát kvôli chybe sanitizačného nástroja pri lepení tagu <style> zo schránky (clipboard). CVE-2020-17017 je chyba neoverenia typu premennej v XPCVariant.cpp, CVE-2020-17024 a CVE-2020-17025 predstavujú chyby pamäte, vrátane jej porušenia s možnosťou vykonávať kód.

Zraniteľné systémy:
Mozilla Firefox verzie staršie ako 72.0.1
Mozilla Firefox ESR verzie staršie ako 68.4.1

Odporúčania:
Odporúčame aktualizáciu na verziu Firefox 72.0.1. resp. Firefox ESR 68.4.1

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-03/

https://www.mozilla.org/en-US/security/advisories/mfsa2020-01/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-02/

Google Chrome

V mesiaci január vydala spoločnosť Google opravu 1 kritickej a 4 závažných zraniteľností.

Kritická zraniteľnosť CVE-2020-6378 a závažná CVE-2020-6379 vzniká v komponente pre rozpoznávanie reči a súvisí s použitím odalokovanej pamäte. Podobnou zraniteľnosťou je CVE-2020-6377, ktorá sa nachádza v audio komponente. Závažná zraniteľnosť CVE-2020-6380 súvisí s chybou overovania správ. Posledná oprava súvisí s ochranou pred zraniteľnosťou CVE-2020-0601 overovania ECC certifikátov v OS Windows.

Zraniteľné systémy:

Google Chrome verzie staršie ako 79.0.3945.130

Odporúčania:

Odporúčame aktualizáciu na verziu 79.0.3945.130

Zdroje:

https://chromereleases.googleblog.com/2020
https://chromereleases.googleblog.com/2020/01/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2020/01/stable-channel-update-for-desktop_16.html

4. Adobe Flash Player, Acrobat a Reader

V mesiaci január nevydala spoločnosť Adobe žiadne opravy pre Flash Player, Acrobat a Reader.

Zdroje:

https://helpx.adobe.com/security.html

5. Frameworky

Microsoft .NET Framework

V mesiaci január boli v .NET Framework opravené 3 kritické zraniteľnosti.

Všetky tri umožňujú vzdialene vykonávať kód. Zraniteľnosti s číslom CVE-2020-0605 a CVE-2020-0606 súvisia s chýbajúcou kontrolou značiek v zdrojovom kóde súboru. Útočník získa práva ako práve prihlásený používateľ a môže inštalovať programy, zobrazovať, meniť a mazať dáta a vytvárať nové používateľské účty. Pre zneužitie zraniteľnosti musí presvedčiť obeť, aby otvorila špeciálne upravený súbor využívajúci zraniteľnú verziu .NET.

Zraniteľnosť CVE-2020-0646 súvisí s nesprávnym vyhodnotením vstupov. Útočník môže získať kontrolu nad systémom a môže inštalovať programy, zobrazovať, meniť a mazať dáta a vytvárať nové používateľské účty. Pre zneužitie zraniteľnosti musí odoslať špecifický vstup do aplikácie využívajúcej zraniteľnú verziu .NET.

Zraniteľné systémy:

Microsoft .NET Framework 3.0 Service Pack 2
Microsoft .NET Framework 3.1
Microsoft .NET Framework 3.5, 3.5.1
Microsoft .NET Framework 4.5.2
Microsoft .NET Framework 4.6, 4.6.1, 4.6.2
Microsoft .NET Framework 4.7, 4.7.1, 4.7.2
Microsoft .NET Framework 4.8

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-2020-0605
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0606
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0646

Oracle Java

Spoločnosť Oracle vydala v mesiaci január plánovanú štvrťročnú veľkú sadu aktualizácií. V produkte Java SE a Java SE Embedded bolo celkovo opravených 12 zraniteľností. Prvé štyri najzávažnejšie sú CVE-2020-2604 s CWE skóre 8.1 a CVE-2020-16168, CVE-2020-13117, CVE-2020-13118 so skóre 7.5.

Zraniteľné systémy:

Java SE: 7u241, 8u231, 11.0.5, 13.0.1
Java SE Embedded: 8u231

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/cpujan2020.html#AppendixJAVA

6. Iné závažné zraniteľnosti

Zraniteľnosť Citrix (Netscaler) ADC a Gateway umožňujúca vzdialene vykonávať kód

Kritická zraniteľnosť zariadení Citrix ADC a Gateway známych aj ako Netscaler umožňuje neautentifikovaným útočníkom vzdialene vykonávať kód po odoslaní špeciálne vytvorenej požiadavky spolu so škodlivým kódom. Verejne dostupné sú minimálne dve funkčné ukážky zneužitia zraniteľnosti. Viac informácií na stránke.

Kritické zraniteľnosti v CMS WordPress doplnkoch InfiniteWP a WP Time Capsule

Dva WordPress doplnky, InfiniteWP a WP Time Capsule, obsahujú závažné bezpečnostné zraniteľnosti, ktoré umožňujú potenciálne obídenie autorizácie administrátora webovej stránky bez potreby použitia prihlasovacieho hesla. Zraniteľné verzie spomenutých doplnkov sa používajú na vyše 320 000 webových stránkach. Viac informácií na stránke.

Internet Explorer zero-day zraniteľnosť spojená so zero-day vo Firefoxe

Spoločnosť Microsoft varuje pred zero-day zraniteľnosťou v prehliadači Internet Explorer CVE-2020-0674. Ponúka a popis zmiernenia následkov, ale záplata zatiaľ neexistuje. Zraniteľnosť umožňuje vzdialené vykonávanie kódu a pravdepodobne je spojená so zero-day zraniteľnosťou CVE-2019-17026 s podobnými následkami v prehliadači Firefox. Verzia prehliadača Firefox 72.0.1 už obsahuje záplatu. Viac informácií na stránke.

Microsoft vydal bezpečnostnú aktualizáciu pre Windows 10, ktorá má odstrániť kritickú zraniteľnosť CryptoAPI. Zasahuje aj Chrome.

Zraniteľnosť CVE-2020-0601, má vplyv na Microsoft Windows CryptoAPI – kryptografické funkcie. Tento komponent je súčasťou jadra operačného systému, ktorý slúži na overovanie kryptografických certifikátov. Zraniteľnosť spôsobuje, že Windows môže chybne overovať nepravé, podvrhnuté certifikáty ako pravé. Útočníci mohli pre užívateľov Windows 10 falšovať aj zabezpečené HTTPS stránky, podvrhnúť škodlivý softvér a vzdialene vykonávať škodlivý kód. Viac informácií na stránke.

Koniec funkcie SHA-1 - nový prakticky realizovateľný kolízny útok

Nový kolízny útok s vybranou predponou, ktorý je možné previesť v praxi s využitím široko dostupných prostriedkov, posiela hašovaciu funkciu SHA-1 ďalej do minulosti. Napriek stále pomerne širokému využitiu je táto funkcia postupne vytláčaná vývojármi a odporúča sa zakázať jej podporu všade, kde je to možné. Viac informácií na stránke.

Nová zraniteľnosť v knižnici OpenSMTPD v operačných systémoch BSD a Linux umožňuje vzdialené vykonanie škodlivého kódu

Zraniteľnosť s označením CVE-2020-7247 môže spôsobiť vykonanie škodlivého kódu s root privilégiami na diaľku cez internet. Zraniteľnosť sa nachádza v knižnici OpenSMTPD v BSD a Linux operačných systémoch. Viac informácií na stránke.