Mesačný prehľad kritických zraniteľností september 2020

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci september 9 kritických a 69 závažných zraniteľností.

Všetky kritické zraniteľnosti opravené v produkte Windows umožňujú vzdialené vykonanie ľubovoľného kódu útočníkom. V produkte bola opravená kritická zraniteľnosť CVE-2020-0908 umožňujúca vzdialené vykonanie kódu, kvôli chybe modulu textovej služby Windows, ktorý nesprávne narába s pamäťou. Útočník, ktorý úspešne zneužije túto chybu, by mohol získať vykonávacie práva v systéme obete.

Ďalšou opravenou bola kritická zraniteľnosť CVE-2020-0922, ktorá spočíva v spôsobe, akým Microsoft COM pre Windows spracováva objekty v pamäti. Útočník, ktorý úspešne zneužije túto chybu, by mohol spustiť ľubovoľný kód v cieľovom systéme.

Opravená bola kritická zraniteľnosť umožňujúca vzdialené vykonanie ľubovoľného kódu CVE-2020-0997 vznikajúca, keď program Windows Camera Codec Pack nesprávne spracováva objekty v pamäti. Útočník, ktorý úspešne zneužije túto chybu, by mohol spustiť ľubovoľný kód v kontexte aktuálneho používateľa. Ak je aktuálny používateľ prihlásený s oprávneniami správcu, útočník by mohol prevziať kontrolu nad systémom a následne inštalovať programy, prezerať, mazať a meniť dáta.

Ďalšou opravenou zraniteľnosťou je CVE-2020-1252, ktorá vzniká keď systém Windows nesprávne narába s objektmi v pamäti a takisto umožňuje vzdialené spustenie kódu. Aby mohol útočník zneužiť túto zraniteľnosť, musel by presvedčiť používateľa, aby spustil špeciálne vytvorenú aplikáciu.

Kritická zraniteľnosť CVE-2020-1285 spočíva v spôsobe, akým rozhranie Windows Graphics Device Interface (GDI) narába s objektmi v pamäti. Útočník, ktorý úspešne zneužije túto chybu, by mohol spustiť ľubovoľný kód a prevziať kontrolu nad postihnutým systémom. Následne by mohol inštalovať programy, prezerať, mazať a meniť dáta.

Kritické zraniteľnosti CVE-2020-1129 a CVE-2020-1139 popisujú zraniteľnosti spočívajúce v spôsobe, akým knižnica Microsoft Windows Codecs Library zaobchádza s objektmi v pamäti. Útočník, ktorý úspešne zneužije túto chybu, by mohol prevziať kontrolu nad postihnutým systémom a následne inštalovať programy, prezerať, mazať a meniť dáta.

Opravené boli aj kritické zraniteľnosti CVE-2020-1508 a CVE-2020-1593, ktoré vznikajú keď program Windows Media Audio Decoder nesprávne spracováva objekty zo vstupu. Útočník, ktorý úspešne zneužije túto chybu, by mohol 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 10 Version 2004 for 32-bit Systems
Windows 10 Version 2004 for ARM64-based Systems
Windows 10 Version 2004 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 1903 (Server Core installation)
Windows Server, version 1909 (Server Core installation)
Windows Server, version 2004 (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-2020-0908
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0922
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0997
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1129
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1252
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1285
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1319
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1508
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1593

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft opravila v mesiaci september 7 kritických a 20 závažných zraniteľností.

Opravené boli kritické zraniteľnosti CVE-2020-1200, CVE-2020-1210, CVE-2020-1452, CVE-2020-1453, CVE-2020-1576 a CVE-2020-1595 v Microsoft SharePoint, kde API nie sú správne chránené pred nebezpečným vstupom od používateľa. To umožňuje vzdialené vykonanie ľubovoľného kódu. Útočník, ktorý úspešne zneužije túto chybu, by mohol vykonať ľubovoľný kód v kontexte aktuálneho používateľa.

Opravená bola aj kritická zraniteľnosť CVE-2020-1460 v serveri Microsoft SharePoint Server, ktorý nedokáže správne identifikovať a filtrovať nebezpečné webové ovládacie prvky ASP.Net. Útočník, ktorý úspešne zneužije túto chybu, by mohol spustiť ľubovoľný kód v kontexte aktuálneho používateľa.

Zraniteľné systémy:

Microsoft Business Productivity Servers 2010 Service Pack 2
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Foundation 2010 Service Pack 2
Microsoft SharePoint Foundation 2013 Service Pack 1

Microsoft SharePoint Server 2010 Service Pack 2
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-2020-1200
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1210
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1452
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1453
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1576
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1595
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1460

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft opravila tento mesiac v prehliadači Internet Explorer 1 kritickú a 2 závažné zraniteľnosti.

Opravená bola kritická zraniteľnosť CVE-2020-0878, ktorá vzniká v spôsobe akým prehliadače Microsoft Internet Explorer pristupujú k objektom v pamäti. Po jej zneužití môže útočník inštalovať programy, prezerať, mazať a meniť dáta alebo si vytvoriť nové účty s plnými užívateľskými právami, alebo spustiť ľubovoľný kód v kontexte aktuálneho používateľa.

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-2020-0878

Microsoft Edge

Spoločnosť Microsoft opravila tento mesiac v prehliadači Microsoft Edge 3 kritické a 1 závažnú zraniteľnosť.

Opravená bola kritická zraniteľnosť CVE-2020-0878, ktorá vzniká v spôsobe akým prehliadače Microsoft Edge pristupujú k objektom v pamäti. Po jej zneužití môže útočník inštalovať programy, prezerať, mazať a meniť dáta alebo si vytvoriť nové účty s plnými užívateľskými právami alebo spustiť ľubovoľný kód v kontexte aktuálneho používateľa.

Ďalšie opravené kritické zraniteľnosti CVE-2020-1057 a CVE-2020-1172 vznikajú v spôsobe akým engine ChakraCore spracúva objekty v pamäti. Útočník by po ich zneužití mohol vykonať ľubovoľný kód v kontexte aktuálneho používateľa.

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-2020-0878
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1057
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1172

Mozilla Firefox

V mesiaci september bola opravená 1 kritická zraniteľnosť v prehliadači Firefox pre Android 80, a to CVE-2020-15664 umožňujúca nalákanie používateľa na inštaláciu nebezpečných rozšírení.

V najnovšej verzii Firefox boli opravené 3 kritické a 3 závažné zraniteľnosti. V najnovšej verzii Firefox ESR boli takisto opravené 3 závažné zraniteľnosti, zatiaľ čo kritická iba jedna. Väčšina

týchto zraniteľností sa týkala chýb umožňujúcich únik údajov z týchto prehliadačov a tiež umožňujúcich predstierať identitu cudzieho zdroja.

Zraniteľné systémy:
Mozilla Firefox verzie staršie ako 81
Mozilla Firefox ESR verzie staršie ako 78.3

Odporúčania:
Odporúčame aktualizáciu Firefox na verziu 81.0.1 resp. Firefox ESR na 78.3.1.

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-39/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-42/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-43/

Google Chrome

V mesiaci september vydala spoločnosť Google opravu 10 závažných zraniteľností svojho prehliadača. Nebola opravená žiadna kritická zraniteľnosť.

Väčšina z opravených závažných zraniteľností vzniká pri nedostatočnej kontrole oprávnení, pri použití odalokovaného miesta v pamäti a pri umožnení zápisu mimo hraníc.

Zraniteľné systémy:
Google Chrome verzie staršie ako 85.0.4183.121

Odporúčania:
Odporúčame aktualizáciu na verziu 85.0.4183.121

Zdroje:
https://chromereleases.googleblog.com/2020
https://chromereleases.googleblog.com/2020/09/stable-channel-update-for-desktop_21.html
https://chromereleases.googleblog.com/2020/09/stable-channel-update-for-desktop.html

4. Adobe Flash Player, Acrobat a Reader

V mesiaci september spoločnosť Adobe nevydala opravu žiadnych kritických zraniteľností pre produkty Adobe Flash Player ani Acrobat a Reader.

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

5. Frameworky

Microsoft .NET Framework

V mesiaci september spoločnosť Microsoft nevydala žiadnu opravnú aktualizáciu pre kritické či závažné zraniteľnosti vo frameworku Microsoft .NET.

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

Oracle Java

Veľká sada opráv je plánovaná na 20. októbra 2020.

Zdroje:
https://www.oracle.com/technetwork/topics/security/alerts-086861.html
https://www.oracle.com/security-alerts/cpujul2020.html#AppendixJAVA

6. Iné závažné zraniteľnosti

Cisco vWAAS obsahuje predvolené statické administrátorské prihlasovacie údaje

Cisco Virtual Wide Area Application Services (vWAAS) je služba na optimalizáciu pre cloudovú infraštruktúru. Táto služba je dodávaná v zariadeniach Cisco s predvolenými statickými údajmi ktoré môže vzdialený neautentifikovaný útočník využiť na prihlásenie sa do administrátorského konta. Viac informácií na stránke.

Expert z Google Project Zero odhalil 3 zraniteľnosti Apache Web Server

Felix Wilhelm z Google Project Zero objavil viacero zraniteľností na webovom serveri Apache. Spoločnosť Apache Foundation vydala záplatu adresovanú týmto zraniteľnostiam, ktoré by mohol potenciálny útočník za určitých podmienok zneužiť na vykonanie ľubovoľného kódu, alebo zapríčinenie nedostupnosti služby (DoS) zlyhaním servera. Viac informácií na stránke.

Cisco Jabber obsahuje kritickú zraniteľnosť umožňujúcu vzdialené vykonávanie kódu

Aplikácia Cisco Jabber obsahuje XSS zraniteľnosť, ktorá sa dá využiť na vzdialené spustenie programov s právami prihláseného používateľa. Na zneužitie zraniteľnosti je potrebné, aby Jabber využíval protokol XMPP s povoleným rozšírením XHTML-IM. Viac informácií na stránke.

Útočníci aktívne zneužívajú zraniteľnosť operačného systému Windows nazvanú „Zerologon“

Spoločnosť Microsoft v auguste 2020 vydala bezpečnostnú aktualizáciu pre 120 zraniteľností operačného systému Windows Server, z ktorých boli dve zero-day. V rámci tejto aktualizácie Microsoft upozorňuje na aktívne zneužívanie kritickej zraniteľnosti nazvanej „Zerologon“. Viac informácií na stránke.