Mesačný prehľad kritických zraniteľností december 2020

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci december 1 kritickú a 21 závažných zraniteľností.

Kritická zraniteľnosť CVE-2020-17095 sa týka Hyper-V. Umožňuje útočníkovi vzdialene vykonávať kód a tiež eskalovať privilégiá. Chyba existuje, keď Windows Hyper-V na hostiteľskom serveri nedokáže správne overiť vstup od autentifikovaného používateľa v hosťovskom operačnom systéme. Na zneužitie tejto zraniteľnosti je postačujúce, aby útočník na hosťovskom systéme Hyper-V spustil špeciálne vytvorenú aplikáciu, ktorá by mohla spôsobiť, že sa v hostiteľskom operačnom systéme Hyper-V vykoná ľubovoľný kód v prípade, že nedokáže správne overiť údaje paketu vSMB.

Väčšina zo závažných zraniteľností môže viesť k eskalácii privilégií. CVE-2020-16958 až CVE-2020-16964 sa vyskytujú vo Windows Backup Engine. Zraniteľnosti CVE-2020-17103, CVE-2020-17134 a CVE-2020-17136 sa nachádzajú v ovládači Windows Cloud Files Mini Filter. CVE-2020-17137 sa vyskytuje v kerneli DirectX Graphics, CVE-2020-17097 v prijímači Windows Digital Media a CVE-2020-17092 v službe Windows Network Connections.

Zneužitím závažných zraniteľností vo Windows Lock Screen, Windows Overlay Filter alebo Kerberos môže dôjsť k obídeniu bezpečnostných prvkov. Zraniteľnosť CVE-2020-17096 vo Windows NTFS môže viesť ku vzdialenému vykonávaniu kódu a umožňuje útočníkom získať vyššie oprávnenia. Zneužitím zraniteľnosti vo Windows SMB, Windows Error Reporting alebo vo Windows GDI+ môže dôjsť k vyzradeniu informácií.

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 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 10 Version 20H2 for 32-bit Systems
Windows 10 Version 20H2 for ARM64-based Systems
Windows 10 Version 20H2 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)
Windows Server, version 20H2 (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-2020-17095

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft opravila v mesiaci december 2 kritické a 12 závažných zraniteľností v kancelárskych balíkoch Microsoft Office a Office Web Apps.

Kritickou zraniteľnosťou je CVE-2020-17121 nachádzajúca sa v produkte Microsoft Sharepoint. Je typu RCE, pričom jej zneužitím je útočník schopný vzdialene vykonávať ľubovoľný .NET kód na postihnutom serveri v kontexte účtu služby Sharepoint Web Application. Kritickou zraniteľnosťou v produkte Microsoft Sharepoint je aj CVE-2020-17118, ktorá tiež umožňuje vzdialené vykonávanie kódu.

Závažné zraniteľnosti v týchto produktoch môžu viesť ku vzdialenému vykonávaniu kódu, k neautorizovanému získaniu vyšších oprávnení, k vyzradeniu informácií alebo k obídeniu bezpečnostných prvkov.

Zraniteľné systémy:

Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Excel 2010 Service Pack 2 (32-bit editions)
Microsoft Excel 2010 Service Pack 2 (64-bit editions)
Microsoft Excel 2013 RT Service Pack 1
Microsoft Excel 2013 Service Pack 1 (32-bit editions)
Microsoft Excel 2013 Service Pack 1 (64-bit editions)
Microsoft Excel 2016 (32-bit edition)
Microsoft Excel 2016 (64-bit edition)
Microsoft Office 2010 Service Pack 2 (32-bit editions)
Microsoft Office 2010 Service Pack 2 (64-bit editions)
Microsoft Office 2016 (32-bit edition)
Microsoft Office 2016 (64-bit edition)
Microsoft Office 2019 for 32-bit editions
Microsoft Office 2019 for 64-bit editions
Microsoft Office 2019 for Mac
Microsoft Office Online Server
Microsoft Office Web Apps 2010 Service Pack 2
Microsoft Office Web Apps 2013 Service Pack 1
Microsoft Outlook 2010 Service Pack 2 (32-bit editions)
Microsoft Outlook 2010 Service Pack 2 (64-bit editions)
Microsoft Outlook 2013 RT Service Pack 1
Microsoft Outlook 2013 Service Pack 1 (32-bit editions)
Microsoft Outlook 2013 Service Pack 1 (64-bit editions)
Microsoft Outlook 2016 (32-bit edition)
Microsoft Outlook 2016 (64-bit edition)
Microsoft PowerPoint 2010 Service Pack 2 (32-bit editions)
Microsoft PowerPoint 2010 Service Pack 2 (64-bit editions)
Microsoft PowerPoint 2013 RT Service Pack 1
Microsoft PowerPoint 2013 Service Pack 1 (32-bit editions)
Microsoft PowerPoint 2013 Service Pack 1 (64-bit editions)
Microsoft PowerPoint 2016 (32-bit edition)
Microsoft PowerPoint 2016 (64-bit edition)
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
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-2020-17118
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-17121

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft neopravila tento mesiac v prehliadači Internet Explorer žiadnu kritickú ani závažnú zraniteľnosť.

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

Microsoft Edge

Spoločnosť Microsoft opravila tento mesiac v prehliadači Microsoft Edge 1 kritickú zraniteľnosť CVE-2020-17131, ktorá sa vyskytuje v skriptovacom engine Chakra a môže viesť k poškodeniu pamäte.

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-2020-17131

Mozilla Firefox

V mesiaci december bola v prehliadači Firefox a Firefox ESR opravená 1 kritická zraniteľnosť. V najnovšej verzii Firefox boli opravené 4 závažné zraniteľnosti, pričom 3 z nich sa vyskytujú aj vo Firefox ESR.

Kritická zraniteľnosť CVE-2020-16042 sa vyskytuje v prehliadači Firefox verzie staršej ako 84, a Firefox ESR verzie staršej 78.6. Operácie nad premennou typu BigInt môžu viesť k odhaleniu neinicializovanej pamäte.

Závažná zraniteľnosť CVE-2020-26971 súvisí s pretečením medzipamäte haldy vo WebGL, CVE-2020-26972 a týka sa použitia odalokovaného miesta v pamäti vo WebGL. CVE-2020-26973 spôsobuje, že CSS Sanitizer môže pri sanitácii odstrániť nesprávne komponenty. CVE-2020-26974 súvisí s nesprávnym pretypovaním objektu „StyleGenericFlexBasis“, čo môže viesť k použitiu odalokovaného miesta v pamäti haldy alebo poškodeniu pamäte.

Zraniteľné systémy:
Mozilla Firefox verzie staršej ako 84
Mozilla Firefox ESR verzie staršej ako 78.6

Odporúčania:
Odporúčame aktualizáciu Firefox na verziu 84 resp. Firefox ESR na 78.6.

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-54/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-55/

Google Chrome

V mesiaci december bola vydaná oprava pre 4 závažné zraniteľnosti. Nebola opravená žiadna kritická zraniteľnosť. CVE-2020-16037, CVE-2020-16038 a CVE-2020-16039 súvisia s použitím odalokovaného miesta v pamäti. CVE-2020-16040 sa týka nedostatočnej validácie dát v komponente V8.

Zraniteľné systémy:
Google Chrome verzie staršej ako 87.0.4280.88 pre Windows, Mac a Linux

Odporúčania:
Odporúčame aktualizáciu na verziu 87.0.4280.88 pre Windows, Mac a Linux.

Zdroje:
https://chromereleases.googleblog.com/2020
https://chromereleases.googleblog.com/2020/12/stable-channel-update-for-desktop.html

4. Adobe Flash Player, Acrobat a Reader

V mesiaci december bola v Adobe Acrobat a Reader opravená 1 závažná zraniteľnosť. Zraniteľnosť CVE-2020-29075 súvisí s nesprávnym overením vstupu a môže viesť k vyzradeniu informácií. Spoločnosť Adobe nevydala opravu žiadnych kritických ani závažných zraniteľností pre Adobe Flash Player.

Zraniteľné systémy:
Acrobat DC
Acrobat Reader DC
Acrobat 2020
Acrobat Reader 2020
Acrobat 2017
Acrobat Reader 2017

Odporúčania:
Odporúčame aktualizáciu:
Acrobat DC na verziu 2020.013.20074
Acrobat Reader DC na verziu 2020.013.20074
Acrobat 2020 na verziu 2020.001.30018
Acrobat Reader 2020 na verziu 2020.001.30018
Acrobat 2017 na verziu 2017.011.30188
Acrobat Reader 2017 na verziu 2017.011.30188

Zdroje:
https://helpx.adobe.com/security.html
https://helpx.adobe.com/security/products/acrobat/apsb20-75.html

5. Frameworky

Microsoft .NET Framework

V mesiaci december 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 19. január 2021.

Zdroje:
https://www.oracle.com/security-alerts/

6. Iné závažné zraniteľnosti

V NAS zariadeniach od spoločnosti QNAP bolo opravených 6 závažných zraniteľností

Štyri zo závažných zraniteľností sa vyskytujú vo vstavanej aplikácii QTS, alebo QuTS hero v NAS zariadeniach. Ďalšia súvisí s aplikáciou Photo Station a posledná s Multimedia Console. Všetky tieto chyby sú typu XSS a umožňujú útočníkom injektovať škodlivý kód do NAS zariadení, čo môže viesť až ku prevzatiu kontroly nad zraniteľným zariadením. Viac informácií na našej stránke.

V softvéri na správu medicínskych zobrazovacích prístrojov spoločnosti GE Healthcare sa vyskytujú 2 kritické zraniteľnosti

Kritické zraniteľnosti súvisia s predvolenými prihlasovacími údajmi do softvéru, ktorý je určený na správu medicínskych zobrazovacích prístrojov. Údaje sú voľne dostupné na internete a môžu byť zneužité na vykonávanie ľubovoľného kódu alebo na spôsobenie nedostupnosti zariadenia. Zneužitím týchto zraniteľností môžu byť taktiež pozmenené citlivé údaje. Viac informácií na našej stránke.

V aplikácii Cisco Jabber bolo nájdených a opravených niekoľko závažných zraniteľností

Nájdené zraniteľnosti sa týkajú aplikácie Cisco Jabber. Tri z nich sú známe už dlhšie, avšak septembrovou aktualizáciou sa ich nepodarilo úplne odstrániť. Kritická zraniteľnosť umožňuje injektovať ľubovoľný skript a následne vzdialene vykonávať ľubovoľný kód. Závažné zraniteľnosti môžu tiež viesť k vzdialenému vykonávaniu kódu, prípadne k úniku citlivých informácií. Nájdené a opravené boli aj stredne závažné zraniteľnosti. Voči týmto chybám je vo všeobecnosti zraniteľný Cisco Jabber pre Windows, MacOS, ale aj pre Android a iOS. Viac informácií na našej stránke.