Mesačný prehľad kritických zraniteľností
február 2020

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci február 6 kritických a 75 závažných zraniteľností.

Opravené boli kritické zraniteľnosti CVE-2020-0681, CVE-2020-0817 a CVE-2020-0734, ktoré umožňujú útočníkom vzdialene vykonávať kód. Nachádzajú sa vo Windows Remote Desktop Client. Ak sa používateľ pripojí k škodlivému serveru, útočník môže na pripojenom počítači vzdialene vykonávať kód. Následne môže inštalovať programy, prezerať, mazať a meniť dáta a vytvárať účty s plnými používateľskými právami.

Kritické zraniteľnosti CVE-2020-0662 a CVE-2020-0729 tiež umožňujú vzdialene vykonávať kód. Zraniteľnosť CVE-2020-0662 sa nachádza v službe zdieľania internetového pripojenia (ICS) ktorá obsahuje zraniteľnosť poškodenia pamäte a útočníkovi umožňuje na serveri spustiť ľubovoľný kód s vyššou úrovňou oprávnení. Zraniteľnosť CVE-2020-0729 môže umožniť vzdialené vykonanie kódu pri spracovávaní súboru s príponou .LNK. Útočník môže zneužitím tejto zraniteľnosti získať rovnaké používateľské práva ako lokálny používateľ.

Zraniteľnosť CVE-2020-0738 sa nachádza vo Windows Media Foundation, ktorý nesprávne spracúva objekty v pamäti. Po jej zneužití môže útočník 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 for 32-bit Systems Service Pack 2
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
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-2020-0662
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0681
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0729
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0734
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0738
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0817

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft opravila v mesiaci január 6 závažných zraniteľností.

Opravené boli zraniteľnosti CVE-2020-0693 a CVE-2020-0694 nachádzajúce sa v Microsoft SharePoint Server. Server bol zraniteľný, pretože nesprávne ošetroval špeciálne vytvorené webové požiadavky. Využitie zraniteľnosti útočníkovi umožnilo vykonať cross-site-scripting (XSS).

Zraniteľnosť CVE-2020-0695 nachádzajúca sa v Office Online Server umožňuje útočníkovi predstieranie iného odosielateľa (spoofing). Útočník môže po zneužití zraniteľnosti čítať obsah ku ktorému nemá oprávnenia a predstierať inú identitu.

Zraniteľnosť CVE-2020-0696 nachádzajúca sa v Microsoft Outlook umožňuje útočníkovi obísť zabezpečenie nesprávnym spracúvaním URI formátov. Útočník nevie zraniteľnosť priamo využiť na vykonanie vzdialeného kódu, vie ju však zneužiť pri spojení s inými zraniteľnosťami.

Ďalšou opravenou zraniteľnosťou je CVE-2020-0697 v úlohe Microsoft Office OlicenseHeartbeat, kde by útočník, ktorý úspešne zneužil túto zraniteľnosť, mohol túto úlohu spustiť ako SYSTÉM.

Poslednou zraniteľnosťou je CVE-2020-0759, nachádzajúca sa v Microsoft Excel. Jej zneužitie umožňuje útočníkovi vzdialene spustiť kód v kontexte aktuálneho používateľa, teda potenciálne aj s administrátorskými právami. Útočník tak môže inštalovať programy, prezerať, mazať a meniť dáta a vytvárať účty s plnými používateľskými právami.

Zraniteľné systémy:

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 2016 for Mac
Microsoft Office 2019 for 32-bit editions
Microsoft Office 2019 for 64-bit editions
Microsoft Office 2019 for Mac
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 SharePoint Enterprise Server 2016
Microsoft SharePoint Server 2013 Service Pack 1
Microsoft SharePoint Server 2019
Office 365 ProPlus for 32-bit Systems
Office 365 ProPlus for 64-bit Systems
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-2020-0693
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0694
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0695
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0696
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0697
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0759

3. Internetové prehliadače

Microsoft Internet Explorer

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

Opravené boli zraniteľnosti CVE-2020-0673 a CVE-2020-0674, ktorých zneužitie umožňujú útočníkovi spustiť kód v kontexte aktuálneho používateľa, teda potenciálne aj s administrátorskými právami. Útočník tak môže inštalovať programy, prezerať, mazať a meniť dáta a vytvárať účty s plnými používateľskými právami.

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-2020-0673
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0674

Microsoft Edge

Spoločnosť Microsoft opravila tento mesiac v prehliadači Microsoft Edge 5 kritických zraniteľností.

Zraniteľnosti CVE-2020-0710 - CVE-2020-0713 a CVE-2020-0767 umožňujú útočníkovi spustiť kód v kontexte aktuálneho používateľa, teda potenciálne aj s administrátorskými právami. Útočník tak môže inštalovať programy, prezerať, mazať a meniť dáta a vytvárať účty s plnými používateľskými právami.

Zraniteľné systémy:
Microsoft Edge 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-2020-0710
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0711
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0712
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0713
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0767

Mozilla Firefox

V mesiaci február boli opravené 3 závažné zraniteľnosti.

Závažná zraniteľnosť CVE-2020-6796 môže spôsobiť poškodenie pamäte modifikovaním zdieľanej pamäte súvisiacej s informáciami o hlásení zlyhania a samotnom zlyhaní. Zraniteľnosti CVE-2020-6800 a CVE-2020-6801 takisto súvisia s poškodením pamäte a môžu byť zneužité na vzdialené spustenie kódu útočníkom.

Zraniteľné systémy:
Mozilla Firefox verzie staršie ako 73
Mozilla Firefox ESR verzie staršie ako 68.5

Odporúčania:
Odporúčame aktualizáciu na verziu 73 resp. Firefox ESR 68.5.

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-05/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-06/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-07/

Google Chrome

V mesiaci február bola vydaná oprava na 2 závažné zraniteľnosti.

Závažná zraniteľnosť CVE-2020-6407 súvisí s prístupom k pamäti v oblasti mimo dosahu a zraniteľnosť CVE-2020-6418 vzniká vo V8 a spočíva v nedostatočnom overení typu premennej pred jej spracovaním (type confusion).

Zraniteľné systémy:
Google Chrome verzie staršie ako 80.0.3987.122

Odporúčania:
Odporúčame aktualizáciu na verziu 80.0.3987.122

Zdroje:
https://chromereleases.googleblog.com/2020

https://chromereleases.googleblog.com/2020/02/stable-channel-update-for-desktop_24.html

4. Adobe Flash Player, Acrobat a Reader

V mesiaci február vydala spoločnosť Adobe opravu 1 kritickej zraniteľnosti pre Adobe Flash Player. V Adobe Acrobat and Reader bolo opravených 12 kritických a 3 závažné zraniteľnosti.

Zraniteľnosť v Adobe Flash Player CVE-2020-3757 spočíva v nedostatočnom overení typu premennej pred jej spracovaním (type confusion) a jej zneužitie umožňuje útočníkom vzdialene vykonávať kód.

Zneužitie kritických zraniteľností, ktoré boli opravené v Adobe Acrobat and Reader môže útočníkom umožniť okrem vzdialeného vykonávania kódu taktiež vyzradenie informácií či zápis do súborového systému.

Zraniteľné systémy:
Adobe Flash Player Desktop Runtime
Adobe Flash Player for Google Chrome
Adobe Flash Player for Microsoft Edge and Internet Explorer 11
Acrobat DC
Acrobat Reader DC
Acrobat 2017
Acrobat Reader 2017
Acrobat 2015
Acrobat Reader 2015

Odporúčania:
Odporúčame aktualizáciu:
Adobe Flash Player Desktop Runtime, Adobe Flash Player for Google Chrome, Adobe Flash Player for Microsoft Edge and Internet Explorer 11 na verziu 32.0.0.330
Acrobat DC, Acrobat Reader DC na verziu 2020.006.20034
Acrobat 2017, Acrobat Reader 2017 na verziu 2017.011.30158
Acrobat 2015, Acrobat Reader 2015 na verziu 2015.006.30510

Zdroje:
https://helpx.adobe.com/security.html
https://helpx.adobe.com/security/products/flash-player/apsb20-06.html
https://helpx.adobe.com/security/products/acrobat/apsb20-05.html

5. Frameworky

Microsoft .NET Framework

V mesiaci február nevydala spoločnosť Microsoft žiadne opravné aktualizácie pre .NET Framework.

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

Oracle Java

Veľká sada opráv je plánovaná na 14. apríla 2020.

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

6. Iné závažné zraniteľnosti

CDPwn - kritické zraniteľnosti Cisco protokolu CDP

Desiatky miliónov zariadení Cisco po celom svete obsahujú kritické zraniteľnosti umožňujúce vzdialené vykonávanie kódu a vyvolanie nedostupnosti služby. Tento súbor piatich zraniteľností bol nazvaný CDPwn, podľa protokolu, v ktorého implementáciách sa nachádzajú. Útočníci môžu okrem iného sledovať komunikáciu, odpočúvať telefóny, exfiltrovať dáta a úplne ovládnuť sieť, nakoľko zraniteľnosti dovoľujú prechádzať do jej iných segmentov. Viac informácií na stránke.

Opravená kritická XSS zraniteľnosť vo WordPress doplnku GDPR Cookie Consent

Spoločnosť WordPress opravila kritickú zraniteľnosť, zatiaľ bez CVE čísla, vo Wordpress doplnku GDPR Cookie Consent, umožňujúcu útočníkovi pozmeniť obsah alebo vložiť škodlivý cross-site scripting (XSS) obsah na webovú stránku obete. Odporúčame aktualizovať doplnok aspoň na verziu 1.8.3. Viac informácií na stránke.

Kritická chyba vo WordPress doplnku od spoločnosti ThemeGrills

Kritická zraniteľnosť nachádzajúca sa vo WordPress doplnku *ThemeGrill Demo Importer* umožňuje útočníkom kompletné vymazanie obsahu celej webovej stránky a automatické prihlásenie do administrátorskému účtu na stránke, ak vymazaná databáza obsahovala účet s názvom "admin". Odporúčame aktualizovať doplnok aspoň na verziu 1.6.2. Viac informácií na stránke.

Milióny počítačov od Dell, HP, Lenovo a možno aj ďalších výrobcov sú zraniteľné voči firmvérovým útokom

Nedostatočné overovanie autenticity firmvérov periférnych zariadení obvykle od dodávateľov tretích strán robí milióny počítačov využívajúcich Windows alebo Linux zraniteľných voči útokom zameraným na infikovanie firmvérov škodlivým kódom. Navyše v niektorých prípadoch nepomôže ani samotná aktualizácia firmvéru. Viac informácií na stránke.

Cisco Smart Software Manager On-Prem má kritickú zraniteľnosť pri overovaní prístupov

Kritická zraniteľnosť služby Cisco Smart Manager On-Prem umožňuje neoprávneným, vzdialeným útočníkom získať prístup k vysoko-privilegovanému účtu a citlivým častiam systému. Zraniteľnosť sa týka systémových účtov, ktoré majú prednastavené a statické heslo a nie sú pod kontrolou systémového administrátora. Úspešné zneužitie povoľuje útočníkovi obdržať práva čítať a zapisovať do systémových súborov a ku konfigurácii zraniteľného zariadenia. Viac informácií na stránke.