Mesačný prehľad kritických zraniteľností
január 2021

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci január 8 kritických a 57 závažných zraniteľností. Všetky kritické zraniteľnosti umožňujú útočníkom vzdialené vykonávanie ľubovoľného kódu.

Zraniteľnosť CVE-2021-1643 súvisí s rozšíreniami HEVC Video. Existuje z dôvodu nedostatočného overenia vstupu dodaného používateľom. Vzdialený útočník môže do aplikácie poslať špeciálne vytvorený vstup a vykonávať ľubovoľný kód v cieľovom systéme.

Opravené boli tiež zraniteľnosti CVE-2021-1658, CVE-2021-1660, CVE-2021-1666, CVE-2021-1667 a CVE-2021-1673, ktoré sa týkajú Remote Procedure Call Runtime a súvisia s nedostatočným overením vstupu.

Zraniteľnosť CVE-2021-1665 taktiež súvisí s nedostatočnou validáciou vstupu dodaného používateľom. Nachádza sa vo Windows GDI+. Útočník je schopný vytvoriť špeciálny vstup, vďaka ktorému môže vzdialene vykonávať ľubovoľný kód.

Posledná kritická zraniteľnosť CVE-2021-1668, s rovnakým dopadom a dôsledkami ako majú ostatné, sa nachádza v Microsoft DTV-DVD Video dekóderi.

Zraniteľné systémy:
HEVC Video Extensions
Microsoft Remote Desktop
Remote Desktop client for Windows Desktop
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 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 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-2021-1643
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-1658
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-1660
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-1665
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-1666
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-1667
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-1668
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-1673

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft opravila v mesiaci január 12 závažných zraniteľností a žiadnu kritickú zraniteľnosť.

Závažné zraniteľnosti CVE-2021-1707, CVE-2021-1711 až CVE-2021-1716 umožňujú útočníkom vzdialené vykonávanie kódu. Zneužitím CVE-2021-1641 a CVE-2021-1717, vyskytujúcich sa v produktoch SharePoint, môže dôjsť k predstieraniu identity, pričom útočník je schopný sfalšovať obsah stránky. CVE-2021-1669 umožňuje obídenie bezpečnostných prvkov a súvisí s použitím vzdialenej plochy. Zraniteľnosti v produkte SharePoint CVE-2021-1712 a CVE-2021-1719 môžu viesť k eskalácii privilégií. Poslednou zraniteľnosťou nachádzajúcou sa v produkte SharePoint je CVE-2021-1718, ktorá môže viesť k neoprávnenej manipulácii na serveri.

Zraniteľné systémy:

Excel Services
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 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 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 Server 2013 Service Pack 1
Microsoft Remote Desktop for Android
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
Microsoft Word 2010 Service Pack 2 (32-bit editions)
Microsoft Word 2010 Service Pack 2 (64-bit editions)
Microsoft Word 2013 RT Service Pack 1
Microsoft Word 2013 Service Pack 1 (32-bit editions)
Microsoft Word 2013 Service Pack 1 (64-bit editions)
Microsoft Word 2016 (32-bit edition)
Microsoft Word 2016 (64-bit edition)
Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Office 2019 for 32-bit editions
Microsoft Office 2019 for 64-bit editions
Microsoft Outlook 2016 (32-bit edition)
Microsoft Outlook 2016 (64-bit edition)
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Foundation 2013 Service Pack 1
Microsoft SharePoint Server 2019
3D Viewer

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

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft neopravila v mesiaci január 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 a žiadnu závažnú zraniteľnosť. Kritická zraniteľnosť CVE-2021-1705 umožňuje vzdialenému útočníkovi získať prístup k potenciálne citlivým informáciám. Existuje z dôvodu okrajovej podmienky v prehliadači 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-2021-1705

Mozilla Firefox

V mesiaci január bola v prehliadači Firefox a Firefox ESR opravená 1 kritická zraniteľnosť. V prehliadači Firefox bolo opravených 5 závažných zraniteľností, pričom 3 z nich sa vyskytujú aj vo Firefox ESR.

Kritická zraniteľnosť CVE-2020-16044 sa týka manipulácie s blokom „COOKIE-ECHO“ v SCTP pakete. Útočník je schopný tento blok upraviť, čo by mohlo viesť k použitiu odalokovaného miesta v pamäti. Pri dostatočnom úsilí by mohol útočník túto chybu zneužiť na vykonávanie ľubovoľného kódu.

Závažné zraniteľnosti vyskytujúce sa v prehliadači Firefox aj Firefox ESR môžu viesť k úniku informácií cez presmerované PDF požiadavky, k poškodeniu pamäte a potenciálnemu zlyhaniu pamäte. Zneužitím zvyšných dvoch zraniteľností, vyskytujúcich sa len v prehliadači Firefox, môže dôjsť k útokom typu „clickjacking“ alebo k poškodeniu pamäte.

Zraniteľné systémy:

Mozilla Firefox verzie staršej ako 85
Mozilla Firefox ESR verzie staršej ako 78.7

Odporúčania:
Odporúčame aktualizáciu Firefox na verziu 85 resp. Firefox ESR na 78.7.

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-01/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-03/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-04/

Google Chrome

V mesiaci január bola vydaná oprava pre 1 kritickú a 21 závažných zraniteľností. Kritická zraniteľnosť CVE-2021-21117 súvisí s nedostatočným presadzovaním politiky v Cryptohome. Závažné zraniteľnosti sa týkajú rôznych komponentov pre prehliadač Chrome. Vo väčšine prípadoch sa jedná o použitie odalokovaného miesta v pamäti, o nedostatočné presadzovanie politiky alebo o nedostatočné overenie údajov.

Zraniteľné systémy:
Google Chrome verzie staršej ako 88.0.4324.96 pre Mac a Linux
Google Chrome verzie staršej ako 88.0.4324.104 pre Windows

Odporúčania:
Odporúčame aktualizáciu na verziu 88.0.4324.96 pre Mac a Linux a na verziu 88.0.4324.104 pre Windows.

Zdroje:
https://chromereleases.googleblog.com/2021
https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html

4. Adobe Flash Player, Acrobat a Reader

V mesiaci január nebola vydaná žiadna oprava pre Adobe Acrobat a Reader. Adobe prestal vydávať záplaty pre Flash Player 31. decembra 2020, teda nie je bezpečné ho používať.

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

5. Frameworky

Microsoft .NET Framework

V mesiaci január 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

Spoločnosť Oracle vydala v mesiaci január plánovanú štvrťročnú veľkú sadu aktualizácií. V produktoch Java SE a Java SE Embedded bola opravená 1 zraniteľnosť. Táto chyba zabezpečenia sa týka nasadení Java, ktoré načítavajú a spúšťajú nedôveryhodný kód, napríklad kód pochádzajúci z internetu.

Zraniteľné systémy:
Java SE: 7u281, 8u271
Java SE Embedded: 8u271

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/cpujan2021.html#AppendixJava

6. Iné závažné zraniteľnosti

V operačnom systéme ThinOS tenkých klientov Dell Wyse sa vyskytujú 2 kritické zraniteľnosti

V operačnom systéme ThinOS na zariadeniach Dell Wyse sa vyskytujú dve kritické zraniteľnosti, ktoré môžu viesť k vzdialenému vykonávaniu škodlivého kódu, prípadne k získaniu neoprávneného prístupu

k ľubovoľným súborom. Zneužitím prvej zraniteľnosti je útočník schopný pristúpiť ku konfiguráciám. Druhá kritická chyba umožňuje nielen čítanie, ale aj zápis do konfiguračných súborov bez autentifikácie. Viac informácií na stránke.

Spoločnosť Zyxel vydala bezpečnostnú aktualizáciu kritickej zraniteľnosti

Výskumný tím Eye Control objavil vo viac ako 100 000 zariadeniach Zyxel nebezpečnú zraniteľnosť. Zariadenia používané ako Firewall, VPN, alebo prístupový bod WLAN obsahujú „zadné vrátka" vo forme účtu určeného pre inštaláciu aktualizácií firmvéru. Tento účet má administrátorské privilégiá a napevno nastavené prihlasovacie údaje. Viac informácií na stránke.

Kritická zero-day zraniteľnosť v Microsoft Windows Defender a ďalších desať v januárovom balíku opráv pre Windows

Spoločnosť Microsoft vydala januárové opravy pre operačné systémy Windows. V balíku 83 aktualizácií sa vyskytuje 11 kritických, z ktorých dve aktívne zneužívané sa nachádzajú vo Windows Defender a ovládači tlačiarní splwow64.exe. Umožňujú vzdialené vykonávanie kódu, falšovanie identity a zvýšenie privilégií. Viac informácií na stránke.

Vážne zraniteľnosti open source softvéru Dnsmasq, ktorý používajú desiatky výrobcov sieťových prvkov

Tím JSOF zverejnil 7 zraniteľností nazvaných DNSpooq. Dnsmasq je open source softvér väčšinou zakomponovaný vo firmvéri sieťových prvkov od všetkých výrobcov. Dnsmasq slúži na preposielanie DNS požiadaviek nadradenému DNS serveru a následnú odpoveď ukladá do medzipamäte DNS, čím zrýchľuje komunikáciu na sieti a predchádza jej zahlcovaniu. Z aktuálne zverejnených 7 zraniteľností sú 4 zraniteľnosti pretečenia medzipamäte a 3 zraniteľnosti umožňujúce otravu záznamov v medzipamäti DNS. Viac informácií na stránke.

NAS zariadenia od spoločnosti QNAP obsahujú 2 kritické zraniteľnosti

Obe kritické zraniteľnosti sa nachádzajú v aplikácii Helpdesk a sú spôsobené nesprávnou kontrolou prístupu. Vzdialený útočník môže zraniteľnosti zneužiť na získanie kontroly nad sieťovými úložnými zariadeniami (NAS). Viac informácií na stránke.