Mesačný prehľad kritických zraniteľností marec 2021

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci marec 6 kritických a 53 závažných zraniteľností. Všetky kritické zraniteľnosti môžu viesť k vzdialenému vykonávaniu kódu.

Zraniteľnosti CVE-2021-24089, CVE-2021-26902 a CVE-2021-27061 sa vyskytujú v rozšíreniach HEVC Video. Všetky súvisia s nesprávnym overením vstupu a môžu viesť k úplnej kompromitácii systému.

Kritická zraniteľnosť CVE-2021-26867 sa nachádza vo Windows Hyper-V. Zraniteľný môže byť každý klient Hyper-V, ktorý je nakonfigurovaný používať Plan 9. Autentifikovaný útočník, ktorý úspešne zneužije túto chybu na klientovi, môže vzdialene vykonávať kód na serveri Hyper-V.

Zraniteľnosť CVE-2021-26876 súvisí s nesprávnym overením vstupu v OpenType Font Parsing. Zraniteľnosť CVE-2021-26897 súvisí s nesprávnym overením vstupu vo Windows DNS serveri. V oboch prípadoch môže vzdialený útočník poslať špeciálne vytvorenú požiadavku a vykonať ľubovoľný kód v cieľovom systéme. Úspešným zneužitím tejto chyby môže dôjsť k úplnej kompromitácii zraniteľného systému.

Zraniteľné systémy:

HEVC Video Extensions
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 Admin Center
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-2021-24089
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-26867
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-26876
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-26897
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-26902
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-27061

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft opravila v mesiaci marec 11 závažných zraniteľností a žiadnu kritickú zraniteľnosť.

Osem zo závažných zraniteľností (CVE-2021-24108, CVE-2021-27053, CVE-2021-27054, CVE-2021-27056 až CVE-2021-27059 a CVE-2021-27076) umožňuje útočníkom vzdialené vykonávanie kódu. Zneužitie zraniteľnosti CVE-2021-24104 umožní útočníkom predstierať cudziu identitu. Zraniteľnosť CVE-2021-27052 v produktoch SharePoint môže viesť k vyzradeniu informácií. Zraniteľnosť CVE-2021-27055 môže umožniť obídenie bezpečnostných prvkov.

Zraniteľné systémy:

Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Business Productivity Servers 2010 Service Pack 2
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 2013 Service Pack 1
Microsoft Office Web Apps Server 2013 Service Pack 1
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 2013 Service Pack 1
Microsoft SharePoint Server 2019
Microsoft Visio 2010 Service Pack 2 (32-bit editions)
Microsoft Visio 2010 Service Pack 2 (64-bit editions)
Microsoft Visio 2013 Service Pack 1 (32-bit editions)
Microsoft Visio 2013 Service Pack 1 (64-bit editions)
Microsoft Visio 2016 (32-bit edition)
Microsoft Visio 2016 (64-bit edition)

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 opravila v mesiaci marec v prehliadači Internet Explorer 1 kritickú a 1 závažnú zraniteľnosť. Kritická 0-day zraniteľnosť CVE-2021-26411, ktorá bola aktívne zneužívaná, môže viesť k poškodeniu pamäte a vzdialenému vykonávaniu kódu. Otvorenie špeciálne vytvoreného HTML súboru môže útočníkovi umožniť spustiť kód na úrovni prihláseného užívateľa v zraniteľnom systéme.

Zraniteľné systémy:
Internet Explorer 11 pre Windows 10
Internet Explorer 11 pre Windows 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-2021-26411

Microsoft Edge

Spoločnosť Microsoft opravila tento mesiac v prehliadači Microsoft Edge 1 kritickú zraniteľnosť. Jedná sa o kritickú zraniteľnosť CVE-2021-26411, ktorá je bližšie popísaná v sekcii o prehliadači Internet Explorer.

Zraniteľné systémy:
Microsoft Edge (EdgeHTML-based)

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-2021-26411

Mozilla Firefox

V mesiaci marec nebola v prehliadači Firefox a Firefox ESR opravená žiadna kritická zraniteľnosť. V prehliadači Firefox ESR boli opravené 3 závažné zraniteľnosti, pričom 2 z nich sa vyskytujú aj v prehliadači Firefox.

Závažná zraniteľnosť CVE-2021-23981 vyskytujúca sa v oboch prehliadačoch môže viesť k poškodeniu pamäte a tiež k potenciálnemu úniku citlivých informácií. Súvisí s čítaním mimo povolených hodnôt. Druhá spoločná zraniteľnosť CVE-2021-23987 tiež môže viesť k poškodeniu pamäte. S dostatočným vynaloženým úsilím by mohol útočník vzdialene vykonávať kód.

Posledný súbor chýb s označením MOZ-2021-0002 v prehliadači Firefox ESR súvisí so zastaralou grafickou knižnicou Angle. Táto knižnica pravdepodobne obsahuje zraniteľnosti, ktoré by mohli byť zneužité.

Zraniteľné systémy:
Mozilla Firefox verzie staršej ako 87
Mozilla Firefox ESR verzie staršej ako 78.9

Odporúčania:
Odporúčame aktualizáciu Firefox na verziu 87 resp. Firefox ESR na 78.9.

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-10/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-11/

Google Chrome

V mesiaci marec bola vydaná oprava pre 17 závažných zraniteľností a žiadnu kritickú. Závažné zraniteľnosti sa väčšinou týkajú pretečenia medzipamäte haldy, použitia odalokovaného miesta v pamäti, nedostatočného overovania dát alebo problému cyklu objektu.

Zraniteľné systémy:
Google Chrome verzie staršej ako 89.0.4389.114 pre Windows, Mac a Linux

Odporúčania:
Odporúčame aktualizáciu na verziu 89.0.4389.114 pre Windows, Mac a Linux.

Zdroje:
https://chromereleases.googleblog.com/2021
https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop_5.html
https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop_12.html
https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop_30.html

4. Adobe Flash Player, Acrobat a Reader

V mesiaci marec nebola opravená žiadna kritická ani závažná zraniteľnosť v produkte 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 marec spoločnosť Microsoft neopravila žiadnu kritickú ani závažnú zraniteľnosť vo frameworku .NET.

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

Oracle Java

Veľká sada opráv je plánovaná na 20. apríl 2021.

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

6. Iné závažné zraniteľnosti

Microsoft vydáva núdzové opravy aktívne zneužívaných zraniteľností serveru Microsoft Exchange

Spoločnosť Microsoft vydala opravné aktualizácie pre kritické zraniteľnosti, ktoré sú aktívne zneužívané útočníkmi pri útokoch na Exchange servery, ktoré sú prevádzkované vo vlastnej infraštruktúre. Spoločnosť Microsoft pripisuje útoky APT skupine s názvom „Hafnium“. Hafnium pravdepodobne zneužíva tieto zraniteľnosti ako súčasť reťazca útokov. Podľa spoločnosti Microsoft útok spočíva v 3 krokoch a to: získanie prístupu na server odcudzením prihlasovacích údajov, alebo zneužitím niektorej zo zraniteľností, následne nasadenie web shellu pre ovládanie cieľového servera a následné odcudzenie údajov cieľových organizácií. Viac informácií na našej stránke.

Spoločnosť VMware opravila kritické zraniteľnosti vo svojich produktoch

Zraniteľnosti sa nachádzajú v systémoch ESXi, vCenter a ich doplnkoch. Týkajú sa všetkých základných inštalácií zraniteľných systémov. Ich úspešným zneužitím môže útočník získať schopnosť vzdialene vykonávať kód a získavať citlivé informácie zo sieťovej infraštruktúry, v ktorej je zraniteľné zariadenie pripojené. VMware odporúča čo najrýchlejšiu aktualizáciu na najnovšie verzie, avšak ak to nie je možné, spoločnosť prišla aj s dočasným riešením zraniteľností na nevyhnutný čas. Viac informácií na našej stránke.

Spoločnosť Cisco opravila 3 kritické zraniteľnosti v rôznych produktoch

Spoločnosť Cisco opravila 3 kritické zraniteľnosti, pričom jedna z nich dosahuje CVSS skóre 10. Táto zraniteľnosť sa nachádza v softvéri ACI Multi-Site Orchestrator. Súvisí s nesprávnou validáciou tokenu v koncovom bode API. Ďalšia chyba sa nachádza v operačnom systéme NX-OS v prepínačoch Nexus. Vzdialený útočník vie manipulovať so súbormi bez akejkoľvek autentifikácie. Posledné zraniteľnosti ovplyvňujú Cisco Application Services Engine. Súvisia s nedostatočnou kontrolou prístupu k službe bežiacej v dátovej sieti. Viac informácií na našej stránke.

V produktoch spoločnosti SAP sa nachádzajú 2 kritické zraniteľnosti

Spoločnosť SAP v rámci marcových bezpečnostných aktualizácií opravila 2 kritické zraniteľnosti. Nachádzajú sa v aplikáciách SAP MII a SAP NetWeaver AS Java. Chyby môžu viesť k vzdialenému vykonávaniu kódu a tiež k úplnej kompromitácii zraniteľného systému. Viac informácií na našej stránke.

Závažná zraniteľnosť v zariadeniach od spoločnosti Apple

Spoločnosť Apple vydala opravu zraniteľnosti CVE-2021-1844, ktorá môže viesť ku vzdialenému vykonávaniu kódu. Chyba sa týka zariadení so systémom iOS, macOS, watchOS a webového prehliadača Safari. Vyskytuje sa vo frameworku WebKit. Používateľom je odporúčané nainštalovať si najnovšie dostupné aktualizácie. Viac informácií na našej stránke.

Spoločnosť F5 varuje pred kritickými zraniteľnosťami svojich produktov

Spoločnosť F5 vydala bezpečnostné aktualizácie svojich produktov, ktoré opravujú kritické zraniteľnosti. Zraniteľnosti by mohli byť zneužité na vzdialené vykonanie kódu (RCE), alebo spôsobenie nedostupnosti služby (DoS). S veľkou váhou apeluje na administrátorov aj organizácia CISA, ktorá upozorňuje na potrebu zabezpečenia produktov spoločnosti F5 pre zamedzenie zneužívania kritických zraniteľností. Viac informácií na našej stránke.

Aktívne zneužívaná kritická zraniteľnosť produktov SonicWall

V produktoch SonicWall Secure Mobile Access 100 (SMA 100) sa nachádza zraniteľnosť typu SQL injection, ktorej zneužitie môže viesť ku neoprávnenému prihláseniu do zariadenia. Produkty SMA 100 sa používajú na vzdialený prístup. Viacero bezpečnostných autorít reportovalo, že je zraniteľnosť aktívne zneužívaná. Z toho dôvodu je potrebné produkty bezodkladne aktualizovať. Viac informácií na našej stránke.

Zraniteľnosti v jadre systému Linux objavené po 15 rokoch

Kyberbezpečnostná spoločnosť GRIMM zverejnila trojicu chýb, ktorú objavila v jadre operačného systému Linux. Zraniteľnosti sa nachádzajú v nepovšimnutom kóde, kde čakali celých 15 rokov. Útočníkom umožňujú eskalovať privilégiá, odcudziť informácie, či spôsobiť nedostupnosť služby. Viac informácií na našej stránke.

V produkte Cisco Jabber bolo opravených 5 zraniteľností

Spoločnosť Cisco vydala záplatu pre 5 zraniteľností vyskytujúcich sa v produkte Cisco Jabber pre Windows, MacOS a mobilné platformy. Kritická zraniteľnosť je spôsobená nesprávnym overovaním obsahu XMPP správy, čo môže viesť ku vzdialenému vykonávaniu kódu. Zneužitím zvyšných 4 chýb

môže dôjsť tiež ku vzdialenému vykonaniu kódu, úniku citlivých informácií alebo narušeniu dostupnosti služby. Viac informácií na našej stránke.

V klientskom softvéri Zoom sa vyskytuje chyba, ktorá môže viesť k odhaleniu citlivých informácií

Vo videokonferenčnej platforme Zoom sa nachádza zraniteľnosť pri zdieľaní obrazovky, ktorej zneužitím môže dôjsť k vyzradeniu citlivých informácií. Chyba zatiaľ nie je opravená, avšak spoločnosť si je vedomá tohto problému a pracuje na jeho vyriešení. Viac informácií na našej stránke.

Kritická zraniteľnosť v knižnici sieťovej masky, npm balíčku Netmask

Victor Viale, Sick Codes, Nick Sahler, Kelly Kaoundis a John Jackson informovali o kritickej zraniteľnosti npm knižnice masky siete, ktorá môže umožniť útočníkovi obísť určité mechanizmy ochrany siete a následne na ňu vykonať útoky. Knižnica npm netmask je využívaná po celom svete a má na konte stovky miliónov stiahnutí. Viac informácií na našej stránke.

Spoločnosť Adobe opravila kritickú zraniteľnosť produktu ColdFusion

Spoločnosť Adobe vydala neplánované bezpečnostné aktualizácie pre produkt ColdFusion verzie 2016, 2018 a 2021. Zraniteľnosť by útočník mohol zneužiť na vzdialené vykonanie ľubovoľného kódu. Viac informácií na našej stránke.

Projekt OpenSSL vydal opravu zraniteľností pre svoju knižnicu zabezpečujúcu šifrovanú komunikáciu

Projekt OpenSSL vydal opravu chýb pre svoju knižnicu, ktorú využívajú mnohé aplikácie a servery na zabezpečenie dôvernej komunikácie. Objavené zraniteľnosti môže útočník zneužiť na spôsobenie nedostupnosti služby, alebo ohroziť dôvernosť a integritu prenášaných dát šifrovaných protokolom TLS. Viac informácií na našej stránke.