CERT BG
COMPUTER EMERGENCY RESPONSE TEAM
BULGARIA

Екип за реагиране при инциденти в компютърната сигурност

Мониторинг на актуалните киберновини – към 15.04.2020 г.

Съдържание

Априлски пач вторник 2020: Microsoft пачва 4 zero-day уязвимости

14 април 2020 г.

Майкрософт публикува 113 пача в голяма актуализация. Той пусна своите актуализации за сигурност в априлския Patch вторник 2020 и това са първите актуализации на пачове, пуснати по време на ерата „работа от вкъщи“ .

От тях 15 са оценени като критични, а 93 - като важни. Най-важното е, че четири от уязвимостите се експлоатират активно; две от тях преди това бяха публично оповестени.

Общо актуализацията включва пачове за Microsoft Windows, Microsoft Edge (базирани на EdgeHTML и базирани на Chromium версии), ChakraCore, Internet Explorer, Microsoft Office и Microsoft Office услуги и уеб приложения, Windows Defender, Visual Studio, Microsoft Dynamics и Microsoft Apps за Android и Mac.

Майкрософт отбелязва 44-процентово годишно увеличение на броя на уязвимостите в периода януари до април, според Trend Micro's Zero Day Initiative (ZDI) - вероятен резултат от нарастващ брой изследователи в сигурността, които търсят грешки и разширяващо се портфолио на поддържаните продукти. През март Patch Tuesday съдържа 115 актуализации; през февруари Microsoft пачва 99 бъга; а през януари той се справя с 50 недостатъка. Те варират от разкриване на информация и ескалация на привилегии до отдалечено изпълнение на код (Remote Code Execution) и cross-site scripting на различни сайтове (XSS).

Потребителите трябва да инсталират тези актуализации за сигурност възможно най-бързо, за да защитят Windows от рискове в сигурността.

Zero-day уязвимости, пачнати през април 2020

- CVE-2020-0935 - OneDrive for Windows Elevation of Privilege Vulnerability
- CVE-2020-1020 - Adobe Font Manager Library Remote Code Execution Vulnerability

- CVE-2020-0938 - Adobe Font Manager Library Remote Code Execution Vulnerability
- CVE-2020-1020 - Adobe Font Manager Library Remote Code Execution Vulnerability

Актуализациите за сигурност, пуснати през април 2020 г.

По-долу е даден пълният списък с пачнати уязвимости и публикувани препоръки в актуализациите на Patch Tuesday от април 2020 г. За достъп до пълното описание на всяка уязвимост и системите, върху които влияят, можете да видите пълния списък тук.

Tag	CVE ID	CVE Title	Severity
Android App	CVE-2020-0943	Microsoft YourPhone Application for Android Authentication Bypass Vulnerability	Important
Apps	CVE-2020-1019	Microsoft RMS Sharing App for Mac Elevation of Privilege Vulnerability	Important
Microsoft Dynamics	CVE-2020-1050	Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability	Important
Microsoft Dynamics	CVE-2020-1018	Microsoft Dynamics Business Central/NAV Information Disclosure	Important
Microsoft Dynamics	CVE-2020-1049	Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability	Important
Microsoft Dynamics	CVE-2020-1022	Dynamics Business Central Remote Code Execution Vulnerability	Critical
Microsoft Graphics Component	CVE-2020-0952	Windows GDI Information Disclosure Vulnerability	Important
Microsoft Graphics Component	CVE-2020-0938	Adobe Font Manager Library Remote Code Execution Vulnerability	Important
Microsoft Graphics Component	CVE-2020-0687	Microsoft Graphics Remote Code Execution Vulnerability	Critical
Microsoft Graphics Component	CVE-2020-0987	Microsoft Graphics Component Information Disclosure Vulnerability	Important
Microsoft Graphics Component	CVE-2020-1004	Windows Graphics Component Elevation of Privilege Vulnerability	Important
Microsoft Graphics Component	CVE-2020-1005	Microsoft Graphics Component Information Disclosure Vulnerability	Important
Microsoft	CVE-2020-	Win32k Elevation of Privilege Vulnerability	Important

Graphics Component	0958		
Microsoft Graphics Component	CVE-2020-0907	Microsoft Graphics Components Remote Code Execution Vulnerability	Critical
Microsoft Graphics Component	CVE-2020-0982	Microsoft Graphics Component Information Disclosure Vulnerability	Important
Microsoft Graphics Component	CVE-2020-0964	GDI+ Remote Code Execution Vulnerability	Important
Microsoft Graphics Component	CVE-2020-1020	Adobe Font Manager Library Remote Code Execution Vulnerability	Important
Microsoft Graphics Component	CVE-2020-0784	DirectX Elevation of Privilege Vulnerability	Important
Microsoft JET Database Engine	CVE-2020-0995	Jet Database Engine Remote Code Execution Vulnerability	Important
Microsoft JET Database Engine	CVE-2020-0999	Jet Database Engine Remote Code Execution Vulnerability	Important
Microsoft JET Database Engine	CVE-2020-0988	Jet Database Engine Remote Code Execution Vulnerability	Important
Microsoft JET Database Engine	CVE-2020-0992	Jet Database Engine Remote Code Execution Vulnerability	Important
Microsoft JET Database Engine	CVE-2020-0994	Jet Database Engine Remote Code Execution Vulnerability	Important
Microsoft JET Database	CVE-2020-0953	Jet Database Engine Remote Code Execution Vulnerability	Important

Engine			
Microsoft JET Database Engine	CVE-2020-0889	Jet Database Engine Remote Code Execution Vulnerability	Important
Microsoft JET Database Engine	CVE-2020-0959	Jet Database Engine Remote Code Execution Vulnerability	Important
Microsoft JET Database Engine	CVE-2020-0960	Jet Database Engine Remote Code Execution Vulnerability	Important
Microsoft JET Database Engine	CVE-2020-1008	Jet Database Engine Remote Code Execution Vulnerability	Important
Microsoft Office	CVE-2020-0979	Microsoft Excel Remote Code Execution Vulnerability	Important
Microsoft Office	CVE-2020-0980	Microsoft Word Remote Code Execution Vulnerability	Important
Microsoft Office	CVE-2020-0984	Microsoft (MAU) Office Elevation of Privilege Vulnerability	Important
Microsoft Office	CVE-2020-0760	Microsoft Office Remote Code Execution Vulnerability	Important
Microsoft Office	CVE-2020-0991	Microsoft Office Remote Code Execution Vulnerability	Important
Microsoft Office	CVE-2020-0961	Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability	Important
Microsoft Office	CVE-2020-0931	Microsoft SharePoint Remote Code Execution Vulnerability	Critical
Microsoft Office	CVE-2020-0906	Microsoft Excel Remote Code Execution Vulnerability	Important
Microsoft Office	CVE-2020-0935	OneDrive for Windows Elevation of Privilege Vulnerability	Important
Microsoft Office SharePoint	CVE-2020-0927	Microsoft Office SharePoint XSS Vulnerability	Critical
Microsoft	CVE-2020-	Microsoft Office SharePoint XSS Vulnerability	Important

Office SharePoint	0923		
Microsoft Office SharePoint	CVE-2020-0925	Microsoft Office SharePoint XSS Vulnerability	Important
Microsoft Office SharePoint	CVE-2020-0924	Microsoft Office SharePoint XSS Vulnerability	Important
Microsoft Office SharePoint	CVE-2020-0932	Microsoft SharePoint Remote Code Execution Vulnerability	Critical
Microsoft Office SharePoint	CVE-2020-0930	Microsoft Office SharePoint XSS Vulnerability	Important
Microsoft Office SharePoint	CVE-2020-0933	Microsoft Office SharePoint XSS Vulnerability	Important
Microsoft Office SharePoint	CVE-2020-0920	Microsoft SharePoint Remote Code Execution Vulnerability	Important
Microsoft Office SharePoint	CVE-2020-0929	Microsoft SharePoint Remote Code Execution Vulnerability	Critical
Microsoft Office SharePoint	CVE-2020-0971	Microsoft SharePoint Remote Code Execution Vulnerability	Important
Microsoft Office SharePoint	CVE-2020-0975	Microsoft SharePoint Spoofing Vulnerability	Important
Microsoft Office SharePoint	CVE-2020-0978	Microsoft Office SharePoint XSS Vulnerability	Important
Microsoft Office SharePoint	CVE-2020-0977	Microsoft SharePoint Spoofing Vulnerability	Important
Microsoft Office SharePoint	CVE-2020-0976	Microsoft SharePoint Spoofing Vulnerability	Important
Microsoft	CVE-2020-	Microsoft SharePoint Remote Code Execution	Critical

Office SharePoint	0974	Vulnerability	
Microsoft Office SharePoint	CVE-2020-0973	Microsoft Office SharePoint XSS Vulnerability	Important
Microsoft Office SharePoint	CVE-2020-0972	Microsoft SharePoint Spoofing Vulnerability	Important
Microsoft Office SharePoint	CVE-2020-0954	Microsoft Office SharePoint XSS Vulnerability	Moderate
Microsoft Office SharePoint	CVE-2020-0926	Microsoft Office SharePoint XSS Vulnerability	Important
Microsoft Scripting Engine	CVE-2020-0968	Scripting Engine Memory Corruption Vulnerability	Moderate
Microsoft Scripting Engine	CVE-2020-0966	VBScript Remote Code Execution Vulnerability	Low
Microsoft Scripting Engine	CVE-2020-0895	Windows VBScript Engine Remote Code Execution Vulnerability	Low
Microsoft Scripting Engine	CVE-2020-0969	Chakra Scripting Engine Memory Corruption Vulnerability	Critical
Microsoft Scripting Engine	CVE-2020-0970	Scripting Engine Memory Corruption Vulnerability	Critical
Microsoft Scripting Engine	CVE-2020-0967	VBScript Remote Code Execution Vulnerability	Moderate
Microsoft Windows	CVE-2020-0942	Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability	Important
Microsoft Windows	CVE-2020-0965	Microsoft Windows Codecs Library Remote Code Execution Vulnerability	Critical
Microsoft Windows	CVE-2020-0940	Windows Push Notification Service Elevation of Privilege Vulnerability	Important
Microsoft	CVE-2020-	Windows Elevation of Privilege Vulnerability	Important

Windows	0934		
Microsoft Windows	CVE-2020-1029	Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability	Important
Microsoft Windows	CVE-2020-1011	Windows Elevation of Privilege Vulnerability	Important
Microsoft Windows	CVE-2020-1094	Windows Work Folder Service Elevation of Privilege Vulnerability	Important
Microsoft Windows	CVE-2020-1016	Windows Push Notification Service Information Disclosure Vulnerability	Important
Microsoft Windows	CVE-2020-0794	Windows Denial of Service Vulnerability	Important
Microsoft Windows	CVE-2020-1017	Windows Push Notification Service Elevation of Privilege Vulnerability	Important
Microsoft Windows	CVE-2020-0944	Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability	Important
Microsoft Windows	CVE-2020-1006	Windows Push Notification Service Elevation of Privilege Vulnerability	Important
Microsoft Windows	CVE-2020-1009	Windows Elevation of Privilege Vulnerability	Important
Microsoft Windows	CVE-2020-0981	Windows Token Security Feature Bypass Vulnerability	Important
Microsoft Windows	CVE-2020-1001	Windows Push Notification Service Elevation of Privilege Vulnerability	Important
Microsoft Windows DNS	CVE-2020-0993	Windows DNS Denial of Service Vulnerability	Important
Open Source Software	CVE-2020-1026	MSR JavaScript Cryptography Library Security Feature Bypass Vulnerability	Important
Remote Desktop Client	CVE-2020-0919	Microsoft Remote Desktop App for Mac Elevation of Privilege Vulnerability	Important
Visual Studio	CVE-2020-0899	Microsoft Visual Studio Elevation of Privilege Vulnerability	Important
Visual Studio	CVE-2020-0900	Visual Studio Extension Installer Service Elevation of Privilege Vulnerability	Important
Windows Defender	CVE-2020-1002	Microsoft Defender Elevation of Privilege Vulnerability	Important

Windows Defender	CVE-2020-0835	Windows Defender Antimalware Platform Hard Link Elevation of Privilege Vulnerability	Important
Windows Hyper-V	CVE-2020-0918	Windows Hyper-V Elevation of Privilege Vulnerability	Important
Windows Hyper-V	CVE-2020-0910	Windows Hyper-V Remote Code Execution Vulnerability	Critical
Windows Hyper-V	CVE-2020-0917	Windows Hyper-V Elevation of Privilege Vulnerability	Important
Windows Kernel	CVE-2020-0699	Win32k Information Disclosure Vulnerability	Important
Windows Kernel	CVE-2020-1027	Windows Kernel Elevation of Privilege Vulnerability	Important
Windows Kernel	CVE-2020-1003	Windows Kernel Elevation of Privilege Vulnerability	Important
Windows Kernel	CVE-2020-0955	Windows Kernel Information Disclosure in CPU Memory Access	Important
Windows Kernel	CVE-2020-1015	Windows Elevation of Privilege Vulnerability	Important
Windows Kernel	CVE-2020-1000	Windows Kernel Elevation of Privilege Vulnerability	Important
Windows Kernel	CVE-2020-1007	Windows Kernel Information Disclosure Vulnerability	Important
Windows Kernel	CVE-2020-0957	Win32k Elevation of Privilege Vulnerability	Important
Windows Kernel	CVE-2020-0936	Windows Scheduled Task Elevation of Privilege Vulnerability	Important
Windows Kernel	CVE-2020-0956	Win32k Elevation of Privilege Vulnerability	Important
Windows Kernel	CVE-2020-0962	Win32k Information Disclosure Vulnerability	Important
Windows Kernel	CVE-2020-0821	Windows Kernel Information Disclosure Vulnerability	Important
Windows Kernel	CVE-2020-0913	Windows Kernel Elevation of Privilege Vulnerability	Important
Windows Kernel	CVE-2020-0888	DirectX Elevation of Privilege Vulnerability	Important
Windows Media	CVE-2020-0948	Media Foundation Memory Corruption Vulnerability	Critical

Windows Media	CVE-2020-0937	Media Foundation Information Disclosure Vulnerability	Important
Windows Media	CVE-2020-0949	Media Foundation Memory Corruption Vulnerability	Critical
Windows Media	CVE-2020-0939	Media Foundation Information Disclosure Vulnerability	Important
Windows Media	CVE-2020-0950	Media Foundation Memory Corruption Vulnerability	Critical
Windows Media	CVE-2020-0946	Media Foundation Information Disclosure Vulnerability	Important
Windows Media	CVE-2020-0947	Media Foundation Information Disclosure Vulnerability	Important
Windows Media	CVE-2020-0945	Media Foundation Information Disclosure Vulnerability	Important
Windows Update Stack	CVE-2020-0996	Windows Update Stack Elevation of Privilege Vulnerability	Important
Windows Update Stack	CVE-2020-1014	Microsoft Windows Update Client Elevation of Privilege Vulnerability	Important
Windows Update Stack	CVE-2020-0983	Windows Elevation of Privilege Vulnerability	Important
Windows Update Stack	CVE-2020-0985	Windows Update Stack Elevation of Privilege Vulnerability	Important

За повече информация:

https://threatpost.com/april-patch-tuesday-microsoft-active-exploit/154794/

https://thehackernews.com/2020/04/windows-patch-update.html

https://www.bleepingcomputer.com/news/microsoft/microsoft-april-2020-patch-tuesday-fixes-3-zero-days-15-critical-flaws/

Adobe поправя важни недостатъци в ColdFusion, After Effects и Digital Edition

14 април 2020 г.

Adobe пусна пачове на уязвимости в своите приложения ColdFusion, After Effects и Digital Editions. Ако бъдат експлоатирани, недостатъците могат да дадат възможност на нападателите да имат достъп до чувствителни данни, да получат ескалирани привилегии и да стартират атаки за отказ от услуга. Всяка от грешките беше оценена като важна въз основа на класациите на CVSS.

Като цяло недостатъците на Adobe, които са поправени в Patch Tuesday, са свързани с пет уязвимости. Този брой е малък в сравнение с март, когато Adobe поправи недостатъци, обвързани с 41 уязвимости в своите продукти, 29 от които са критични по тежест. През февруари Adobe проправи недостатъци, обвързани с 42 уязвимости в своите редовно планирани актуализации, 35 от които бяха критични по тежест.

Три от уязвимостите, разкрити тази седмица, бяха открити в ColdFusion, платформата за бързо разработване на уеб приложения на Adobe. Тези недостатъци включват недостатък на валидиране на входа (CVE-2020-3767), който може да позволи отказ от услуга на ниво приложение (DoS), DLL search-order hijacking glitch (CVE-2020-3768), който може да позволи ескалация на привилегиите и неправилен контрол на достъпа (CVE-2020-3796), което може да доведе до разкриване на структурата на системните файлове.

Засегнати са Актуализация 14 и по-ранна версия на ColdFusion 2016 (потребителите се насърчават да актуализират до актуализация 15) и актуализация 8 и по-ранна версия на ColdFusion 2018 (фиксирана в актуализация 9). Тези недостатъци имат рейтинг на актуализация по приоритет 2, което означава, че недостатъците са открити в продукт, „който в исторически план е бил с повишен риск“ - но „понастоящем няма известни експлоатации“, според Adobe.

Adobe отстрани и недостатъка за разкриване на информация в Adobe After Effects, в неговите цифрови визуални ефекти, графики за движение и приложение за композиране за Windows. Уязвимостта е CVE-2020-3809. Този недостатък позволява на отдалечени атакуващи да разкриват чувствителна информация за засегнатите инсталации на Adobe After Effects. За да се използва тази уязвимост е необходимо взаимодействие с потребителя, като мишената трябва да посети злонамерена страница или да отвори злонамерен файл.

Засегнати са After Effects версии 17.0.1 и по-стари; поправка е налична във версии 17.0.6 за Windows и macOS.

Друг недостатък, разкрит в Adobe Digital Editions, е неговата програма за четене на електронни книги, която може да даде възможност за разкриване на информация. Тази уязвимост (CVE-2020-3798) произтича от номерацията на файлове (хост или локална мрежа). Засегнати са версии на Digital Editions 4.5.11.187212 и по-нови версии за Windows; потребителите се насърчават да актуализират до версия 4.5.11.187303.

За повече информация:

https://threatpost.com/adobe-fixes-important-flaws-in-coldfusion-after-effects-and-digital-editions/154780/