CERT BG
COMPUTER EMERGENCY RESPONSE TEAM
BULGARIA

Екип за реагиране при инциденти в компютърната сигурност

Мониторинг на актуалните киберновини – към 13.05.2020 г.

Съдържание

Microsoft адресира 111 бъга в майския пач вторник

12 май 2020 г.

Важните недостатъци, свързани с EoP (elevation-of-privilege – ескалация на привилегии) съставляват по-голямата част от уязвимостите; SharePoint продължава критичното си изпълнение с четири тревожни грешки.

Microsoft пусна корекции на 111 уязвимости в сигурността в актуализацията си на майския пач вторник, включително на 16 критични грешки и на 96, които са оценени като важни.

За разлика от други скорошни месечни актуализации на Microsoft тази година, нито един от недостатъците не е публично известен или под активна атака към момента.

Наред с актуализациите на операционна система, браузър, Office и SharePoint, Microsoft пусна и актуализации за .NET Framework, .NET Core, Visual Studio, Power BI, Windows Defender и Microsoft Dynamics.

Бъгове с ескалация на привилегии

По-голямата част от поправките са на важни грешки, свързани с ескалация на привилегии (EoP). В майската версия на Microsoft има общо 56 от тези видове поправки, които засягат различни компоненти на Windows. Този клас уязвимости се използват от нападателите, след като те успеят да получат първоначален достъп до система, за да изпълнят код на целевите системи с повишени привилегии.

Три от тези бъга са получили рейтинг „по-вероятна експлоатация”: Два недостатъка са в Win32k (CVE-2020-1054, CVE-2020-1143) и един в Windows Graphics Component (CVE-2020-1135).

И двата недостатъка в Win32k съществуват, когато kernel-mode драйвърът на Windows не успява да обработва правилно обекти в паметта. Нападател, който успешно е използвал тази уязвимост, може да пусне произволен код вkernel-mode; по този начин, нападателят може да инсталира програми; да разглежда, променя или изтрива данни; или да създава нови акаунти с пълни права на потребители.

За да ги използва, нападателят първо трябва да влезе в системата. След това той може да стартира специално създадено приложение, което да използва уязвимостта и да поеме контрола върху засегнатата система.

Междувременно грешката EoP в Windows Graphics се намира в повечето надстройки на Windows 10 и Windows Server. Уязвимостта може да позволи експлоатация, използваща възможността на Windows Graphics да борави с обекти в паметта. Нападателят може да използва тази уязвимост, за да повиши привилегиите на процеса, позволявайки на атакуващия да открадне идентификационни или чувствителни данни, да изтегли допълнителен зловреден софтуер или да изпълни злонамерен код.

И в Microsoft Edge има и една критична грешка в EoP (CVE-2020-1056). Тя съществува, защото Edge не прилага правилно cross-domain политиките, което би могло да позволи на атакуващ да получи достъп до информация от един домейн и да го инжектира в друг домейн. Въпреки това, във всички случаи атаката изисква взаимодействие с потребителя, като потребителите биват подтиквани да щракнат върху връзка, която ги отвежда до сайта на нападателя.

При уеб базиран сценарий на атака, един нападател може да хоства уебсайт, който се използва за опит за използване на уязвимостта. Освен това компрометираните уебсайтове и уебсайтовете, които приемат или хостват предоставено от потребителите съдържание, могат да съдържат специално изработено съдържание, което да използва уязвимостта.

Пачове на критични уязвимости

Другите бъгове включват два недостатъка на изпълнение на отдалечен код (RCE) в Microsoft Color Management (CVE-2020-1117) и Windows Media Foundation (CVE-2020-1126), които биха могли да бъдат експлоатирани чрез подтикване на потребител чрез техники за социално инженерство да отвори злонамерен прикачен файл в имейл или да посети уебсайт, който съдържа кода на експлоатацията.

Успешната експлоатация би позволила на атакуващ да извърши действия върху системата, използвайки същите права като потребителя, който е компрометиран. Ако потребителят има администраторски привилегии, нападателят може да извърши различни действия, като например инсталиране на програми, създаване на нов акаунт с пълни права и преглед, промяна или изтриване на данни.

Критичните недостатъци включват и актуализации за Chakra Core, Internet Explorer и EdgeHTML, докато SharePoint има четири критични грешки, продължавайки да води в тази категория от миналия месец.

Повечето критичните уязвимости биват пачнати от актуализациите на операционната система и браузъра, но има четири критични уязвимости в SharePoint и една във Visual Studio.

В SharePoint CVE-2020-1023 и CVE-2020-1102 са критични RCE (Remote Code Execution) уязвимости, които биха позволили на нападателите да получат достъп до система и да четат или изтриват съдържание, да правят промени или директно да стартират код в системата.

На атакуващите се дава бърз и лесен достъп не само до най-критичните данни на организацията, съхранявани на SQL сървъра, но и платформа за извършване на допълнителни злонамерени атаки срещу други устройства във вътрешната среда. На системи като SharePoint често е трудно да бъдат приложени пачове офлайн, което позволява на RCE уязвимостите да се задържат във вътрешната инфраструктура. Това дава възможност на нападателите да се движат лесно странично, след като получат достъп.

Пак в SharePoint, CVE-202-1024 позволява на атакуващия да изпълнява произволен код от пула за приложения на SharePoint и farm акаунта на SharePoint сървъра, потенциално въздействащ върху всички потребители, свързани в и използващи платформата.

Що се отнася до Visual Studio, „потребителите на Visual Studio Code Python трябва да вземат под внимание двата пача, пуснати този месец. Единият е оценен като критичен [CVE-2020-1192], а другият като важен [CVE-2020-1171]. Няма индикации защо единият е с по-голяма тежест от другия и потребителите трябва да се отнасят и към двата като към критични.

Други бъгове

Администраторите трябва да обърнат внимание и на други проблеми като два за VBScript (CVE-2020-1060 и CVE-2020-1058).

При експлоатация и двата могат да позволят на нападателя да получи същите права като текущия потребител.

Докато и CVE-2020-1058, и CVE-2020-1060 не са оценени като критични по тежест, много е вероятно те да се използват от нападатели.

Има и интересна уязвимост за отказ от услуга (CVE-2020-1118) в Microsoft Windows Transport Layer Security.

Microsoft напоследък е в процес на отстраняване на бъгове; този месец отбелязва три месеца подред, в които е пуснала пачове за повече от 110 уязвимости.

За повече информация:

https://threatpost.com/microsoft-111-bugs-may-patch-tuesday/155669/

Adobe елиминира 16 критични недостатъка в Acrobat и Reader и в Digital Negative SDK

12 май 2020

Adobe е отстранила 16 критични недостатъка в Acrobat и Reader и в своя Adobe Digital Negative (DNG) Software Development Kit. Ако бъдат експлоатирани, недостатъците могат да доведат до отдалечено изпълнение на код.

Като цяло Adobe фиксира уязвимости, обвързани с 36 CVE. Те включват 24 недостатъка с критична и значителна тежест в Acrobat и Reader, използван за създаване и управление на PDF файлове, и 12 в Adobe Digital Negative (DNG) Software Development Kit, който осигурява поддръжка за четене и запис на DNG файлове, използвани за цифрова фотография.

Adobe не е запознат да е експлоатиран никой от проблемите, адресирани в тези актуализации.

Acrobat и Reader

Дванадесет критични недостатъка бяха отстранени в Acrobat и Reader. По-голямата част от тях, ако бъдат експлоатирани, могат да позволят на атакуващ да започне атаки за изпълнение на произволен код.

Засегнати са Acrobat и Reader DC Continuous версии 2020.006.20042 и по-стари; Версии Acrobat и Reader Classic 2017 версии 2017.011.30166 и по-стари; и Acrobat и Reader Classic 2015 версии 2015.006.30518 и по-стари.

Adobe пусна миналата седмица предварително уведомление за актуализациите на Acrobat и Reader.

Adobe DNG SDK

Adobe пусна и пачове за недостатъци във версии 1.5 и по-ранна версия на своя DNG SDK. Призовават се потребителите да актуализират до версия 1.5.1 на SDK.

През април Adobe пусна пачове за сигурност за уязвимости в своите приложения ColdFusion, After Effects и Digital Editions. Ако бъдат експлоатирани, недостатъците могат да дадат възможност на нападателите да виждат чувствителни данни, да получат ескалирани привилегии и да стартират атаки за отказ от услуга. През април Adobe пусна и пач, адресиращ критични недостатъци в Adobe Bridge, Adobe Illustrator и платформата за електронна търговия Magento. Ако бъдат експлоатирани, най-тежките уязвими места могат да дадат възможност за отдалечено изпълнение на код на засегнатите системи.

За повече информация:

https://threatpost.com/adobe-kills-16-critical-flaws-in-acrobat-and-reader-digital-negative-sdk/155652/