CERT BG
COMPUTER EMERGENCY RESPONSE TEAM
BULGARIA

Екип за реагиране при инциденти в компютърната сигурност

Мониторинг на актуалните киберновини – към 17.07.2020 г.

Съдържание

Adobe пусна юлските пачове на критични уязвимости

14 юли 2020 г.

Adobe пусна актуализации на софтуера, за да закърпи общо 13 нови уязвимости в сигурността, засягащи 5 от широко използваните му приложения.

От тези 13 уязвимости четири са оценени като критични, а девет са важни по тежест.

Засегнатите продукти, които получиха пачове за сигурност, включват:

Adobe Creative Cloud Desktop

Adobe Media Encoder

Adobe GenuineService

Adobe ColdFusion

Adobe Download Manager

Adobe Creative Cloud Desktop Application версии 5.1 и по-стари за операционните системи Windows съдържат четири уязвимости, едната от които е критичен проблем със символна връзка (CVE-2020-9682), водеща до произволни атаки при запис във файловата система.

Според препоръките, другите три важни недостатъка в този софтуер на Adobe са проблеми с ескалацията на привилегии.

Adobe Media Encoder съдържа две критични произволни изпълнения на код (CVE-2020-9650 и CVE-2020-9646) и един важен проблем с разкриването на информация, засягащ както Windows, така и потребители на macOS, работещи с Media Encoder версия 14.2 или по-ранна.

Adobe Genuine Service - помощна програма в Adobe Suite, която не позволява на потребителите да стартират неоригинален или кракнат пиратски софтуер, е засегната от три важни проблема с ескалацията на привилегии. Тези недостатъци се намират в софтуерна версия 6.6и по-ранна за Windows и macOS операционни системи.

Платформата за разработка на уеб приложения на Adobe ColdFusion също страда от два важни проблема за ескалация на привилегиите, които могат да бъдат използвани за отвличане на поръчки за търсене на DLL.

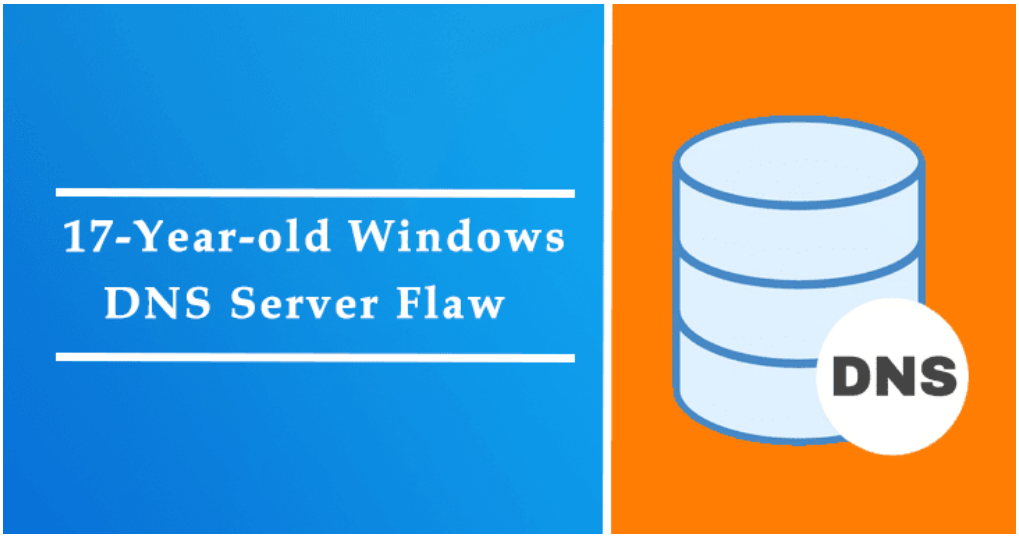
Adobe Download Manager има един недостатък (CVE-2020-9688), който е критичен по тежест и може да доведе до произволно изпълнение на код в текущия потребителски контекст чрез инжектиране на команда. Недостатъкът засяга Adobe Download Manager версия 2.0.0.518 за Windows и е пачнат с издаването на версия 2.0.0.529 на софтуера.

Нито една уязвимост, фиксирана в тази партида от актуализации на Adobe, не е публично оповестена или открита, че се използва. Въпреки това все още се препоръчва на потребителите на Adobe да изтеглят и инсталират най-новите версии на засегнатия софтуер, за да защитят своите системи и организации от потенциални кибератаки.

За повече информация:

https://thehackernews.com/2020/07/adobe-security-patch-july.html

Microsoft пачва критична грешка в Windows DNS сървър, съществуваща от 17 години, която засяга версиите на Windows Server 2003 до 2019 г.



15 юли 2020 г.

Microsoft закърпи критична 17-годишна уязвимост с Windows DNS Server, която може да бъде предизвикана от нападател със злонамерен DNS отговор.

Windows DNS сървърът е съществена част от средата на Windows Domain и изпълнява DNS заявки на Windows Server.

Уязвимостта, наречена SIGRed (CVE-2020-1350), е работеща и получава базов резултат CVSS 10/10 и може да бъде предизвикана от нападател със злонамерен DNS отговор.

Проблемът със защитата на DNS на Windows е открит от Check Point и докладван на Microsoft още през май. Сега пачът е наличен за поддържани версии на Windows сървъри.

Изследователите откриха Hepp-based Integer Overflow „dns.exe! SigWireRead“, с функция, която анализира SIG заявките.

Като изпратим DNS отговор, който съдържа голям (по-голям от 64KB) запис SIG, можем да предизвикаме контролиран buffer overflow.

За да задействат изследователите уязвимостта, първо изпращат 65535 байта DNS съобщение, но откриват, че едно DNS съобщение, ограничено само до 512 байта, не може да я задейства.

Експлоатация от разстояние

Уязвимостта може да се задейства дистанционно чрез HTTP payload, изпращайки я до целевия DNS сървър на порт 53, кара DNS сървъра на Windows да интерпретира този payload, сякаш е DNS заявка.

При популярните сървъри като Google Chrome и Mozilla Firefox не се позволява DNS заявка през порт 53, така че уязвимостта би могла да се експлоатира с браузъри, базирани на Chromium, като Internet Explorer и Microsoft Edge.

Microsoft управлява както DNS клиента, така и DNS сървъра в два различни модула, но уязвимостта остава само при DNS сървъра, тъй като клиентската версия не валидира Sig_RecordRead + D0.

Уязвимостта е оценена със силна тежест и шансът за експлоатация е голям. Успешната експлоатация на тази уязвимост би имала сериозно въздействие.

На потребителите се препоръчва да пачнат засегнатите Windows DNS сървъри, за да предотвратят използването на тази уязвимост.

Като временно решение Check Point предлага да настроите максималната дължина на DNS съобщение (над TCP) на 0xFF00, което би трябвало да премахне уязвимостта.

reg add
“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters
” /v “TcpReceivePacketSize” /t REG_DWORD /d 0xFF00 /fnet stop DNS && net
start DNS

Microsoft пусна пачове на уязвимостта на SIGRed и съветва потребителите незабавно да ги приложат. Ако има активирани автоматични актуализации, тогава не се изискват действия от страна на потребителя.

За повече информация:

https://gbhackers.com/windows-dns-server/