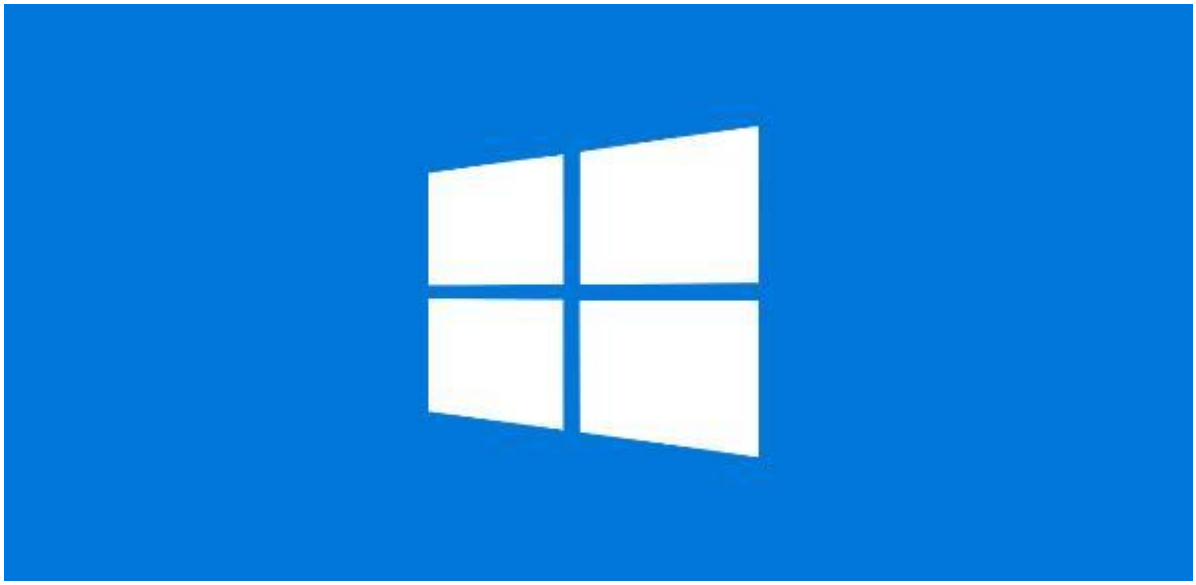
Представлена первая PoC-атака с эксплуатацией уязвимости в Windows



Речь идет об уязвимости CVE-2020-0601 в криптографической библиотеке crypt32.dll в Windows, позволяющей подписывать вредоносные файлы таким образом, чтобы система принимала их за легитимные, а также подделывать цифровые сертификаты. Проблема была обнаружена специалистами Агентства национальной безопасности США, сообщившими о ней Microsoft.

В среду, 15 января, исследователь безопасности Салим Рашид опубликовал в Twitter скриншот, на котором видно, как музыкальное видео Never Gonna Give You Up популярного певца 1980-х Рика Эстли играет на сайтах Github.com и NSA.gov. С помощью уязвимости исследователю удалось осуществить в браузерах Edge и Chrome спуфинг сайтов Github и АНБ США.

Созданный Рашидом эксплоит состоит из 100 строк кода, однако его можно легко сжать до 10 строк, если урезать «несколько полезных фишек», сообщил исследователь изданию Ars Technica.

Хотя проэксплуатировать уязвимость не так-то просто, и для осуществления атаки требуется соблюдение ряда условий, АНБ назвало ее высокоопасной. Другие ИБ-эксперты разделяют мнение коллег из АНБ. «Вот что Салим только что продемонстрировал: с помощью [короткого] скрипта можно создать сертификат для любого сайта, и он будет доверенным в IE и Edge при стандартных настройках Windows. Это ужасно. Проблема затрагивает VPN-шлюзы, VoIP, практически все, что использует сетевые коммуникации», - сообщил руководитель отдела безопасности MongoDB Кенн Уайт (Kenn White).

Источник: https://www.securitylab.ru/news/504149.php