НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200117.2 | 17 января 2019 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Уязвимость в криптографической библиотеки ОС Windows

Идентификатор уязвимости	MITRE: CVE-2020-0601
Идентификатор программной ошибки	CWE-295: Некорректная проверка сертификатов
Описание уязвимости	Эксплуатация уязвимости позволяет злоумышленнику выполнить атаку «человек посередине», а так же обойти проверку подлинности исполняемого файла путем подмены сертификата шифрования на основе эллиптических кривых (ECC). Уязвимость обусловлена некорректной работой механизма проверки сертификатов и криптографических сообщений в Microsoft CryptoAPI.
Категория уязвимого продукта	Операционные системы Windows и их компоненты
Уязвимое ПО	Microsoft Windows 10 x64-x86 Microsoft Windows 10 x64-x86 версии 1607 Microsoft Windows 10 x64-x86 версии 1709 Microsoft Windows 10 x64-x86 версии 1803 Microsoft Windows 10 x64-x86 версии 1809 Microsoft Windows 10 x64-x86 версии 1903 Microsoft Windows 10 x64-x86 версии 1909 Microsoft Windows server 2016 Microsoft Windows server 2019 Microsoft Windows server версии 1803 Microsoft Windows server версии 1903 Microsoft Windows server версии 1909
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	14 января 2020 г.
Дата обновления	16 января 2020 г.

Оценка критичности уязвимости (CVSSv3)	8.1 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Требуется (R)
Масштаб последствий эксплуатации уязвимости (S)	Изменяется (U)
Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Отсутствует (N)
Степень зрелости доступных средств эксплуатации (E)	Концептуальное подтверждение (P)
Наличие средств устранения уязвимости (RL)	Официальное решение (O)
Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)
Ссылки на источники	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0601