

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200514.2 | 14 мая 2020 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Отказ в обслуживании в Microsoft Windows Transport Layer Security

Идентификатор уязвимости	MITRE: CVE-2020-1118
Идентификатор программной ошибки	CWE-20: Некорректная проверка входных данных
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально созданного вредоносного запроса по протоколу TLS до v1.2. Уязвимость обусловлена некорректной работой механизма обмена ключами в Transport Layer Security (TLS) в ОС Windows.
Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
Уязвимое ПО	Windows: 10 1709, 10 1803, 10 1809, 10 1903, 10 1909 Windows Server: 1803, 1903, 1909, 2019
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	12 мая 2020 г.
Дата обновления	12 мая 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)
Масштаб последствий эксплуатации уязвимости (S)	Изменяется (C)
Влияние на конфиденциальность (C)	Отсутствует (N)

Влияние на целостность (I)

Отсутствует (N)

Влияние на доступность (A)

Высокое (H)

Степень зрелости доступных средств эксплуатации

Наличие не подтверждено

Наличие средств устранения уязвимости

Официальное решение

Достоверность сведений об уязвимости

Сведения подтверждены

Ссылки на источники

<https://www.cybersecurity-help.cz/vdb/SB2020051268>

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1118>