

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200611.9 | 11 июня 2020 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Выполнение произвольного кода в Microsoft Browser

Идентификатор уязвимости	MITRE: CVE-2020-1219
Идентификатор программной ошибки	CWE-119: Выполнение операций за пределами буфера памяти
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код на целевом устройстве, вынудив пользователя открыть специально сформированную web-страницу. Уязвимость обусловлена некорректным определением границ буфера памяти при обработке переменных типа Intl в JavaScript.
Категория уязвимого продукта	Операционные системы Microsoft и их компоненты ChakraCore
Уязвимое ПО	Microsoft Edge Microsoft Internet Explorer: 11
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	9 июня 2020 г.
Дата обновления	10 июня 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:N/AC:L/PR:N/UI:R/S:U/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)	Требуется (R)
Масштаб последствий эксплуатации уязвимости (S)	Не изменяется (U)

Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Высокое (H)
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1219>
<https://www.zerodayinitiative.com/advisories/ZDI-20-698/>
<https://www.cybersecurity-help.cz/vdb/SB2020060954>