

# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: [cert.gov.ru](http://cert.gov.ru)  
E-mail: [threats@cert.gov.ru](mailto:threats@cert.gov.ru)

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210714.8 | 14 июля 2021 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

## Выполнение произвольного кода в Windows Scripting Engine

Идентификатор уязвимости	MITRE: CVE-2021-34448
Идентификатор программной ошибки	CWE-119: Выполнение операций за пределами буфера памяти
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированной вредоносной веб-страницы. Уязвимость обусловлена некорректной обработкой HTML данных в обработчике сценариев Windows.
Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
Уязвимый продукт	Windows: 7, 8.1, 10, 10 20H2, 10 21H1, 10 1507, 10 1511, 10 1607, 10 1703, 10 1709, 10 1803, 10 1809, 10 1903, 10 1909, 10 2004, 10 Gold, 10 Mobile, 10 S, RT 8.1 Windows Server: 2008 R2, 2012, 2012 R2, 2016, 2019, 2019 20H2, 2019 1709, 2019 1803, 2019 1903, 2019 1909, 2019 2004 Microsoft Internet Explorer: 11
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	13 июля 2021 г.
Дата обновления	13 июля 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N
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	Высокая
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	<a href="https://www.cybersecurity-help.cz/vdb/SB2021071323">https://www.cybersecurity-help.cz/vdb/SB2021071323</a> <a href="https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34448">https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34448</a>