

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210422.3 | 22 апреля 2021 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Выполнение произвольного кода в ПО компании Mozilla

Идентификатор уязвимости	MITRE: CVE-2021-23994
Идентификатор программной ошибки	CWE-787: Запись за границами буфера
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти при обработке входных данных в буфере кадра WebGL.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Mozilla Firefox: 8.0.1, 60.0, 60.0.1, 60.0.2, 60.1.0, 60.2.0, 60.2.1, 60.2.2, 60.3.0, 60.4.0, 60.5.0, 60.5.1, 60.5.2, 60.6.0, 60.6.1, 60.6.2, 60.6.3, 60.7.0, 61.0, 61.0.1, 61.0.2, 62.0, 62.0.1, 62.0.2, 62.0.3, 63.0, 63.0.1, 63.0.3, 64.0, 64.0.1, 64.0.2, 65.0, 65.0.1, 65.0.2, 66.0, 66.0.1, 66.0.2, 66.0.3, 66.0.4, 66.0.5, 67.0, 67.0.1, 67.0.2, 67.0.3, 67.0.4, 68.0, 68.0.1, 68.0.2, 69.0, 69.0.1, 69.0.2, 69.0.3, 70.0, 70.0.1, 71.0, 72.0, 72.0.1, 72.0.2, 73.0, 73.0.1, 74.0, 74.0.1, 75.0, 76.0, 76.0.1, 77.0, 77.0.1, 78.0, 78.0.1, 78.0.2, 79.0, 80.0, 80.0.1, 81.0, 81.0.1, 81.0.2, 82.0, 82.0.1, 82.0.2, 82.0.3, 83.0, 84.0, 84.0.1, 84.0.2, 85.0, 85.0.1, 85.0.2, 86.0, 86.0.1, 87.0 Firefox ESR: 60.0, 60.0.1, 60.0.2, 60.1.0, 60.2.0, 60.2.1, 60.2.2, 60.3.0, 60.4.0, 60.5.0, 60.5.1, 60.5.2, 60.6.0, 60.6.1, 60.6.2, 60.6.3, 60.7.0, 60.7.1, 60.7.2, 60.8.0, 60.9.0, 68.0, 68.0.1, 68.0.2, 68.1.0, 68.2.0, 68.3.0, 68.4.0, 68.4.1, 68.4.2, 68.5.0, 68.6.0, 68.6.1, 68.7.0, 68.8.0, 68.9.0, 68.10.0, 68.11.0, 68.12.0, 78.0, 78.0.1, 78.0.2, 78.1.0, 78.2.0, 78.3.0, 78.3.1, 78.4.0, 78.4.1, 78.5.0, 78.6.0, 78.6.1, 78.7.0, 78.7.1, 78.8.0, 78.9.0 Mozilla Thunderbird: 60.0, 60.2.1, 60.3, 60.3.0, 60.3.1, 60.3.2, 60.3.3, 60.4, 60.4.0, 60.5, 60.5.0, 60.5.1, 60.5.2, 60.5.3, 60.6.0, 60.6.1, 60.7.0, 60.7.1, 60.7.2, 60.8.0, 60.9.0, 60.9.1, 68.0,

68.1.0, 68.1.1, 68.1.2, 68.2.0, 68.2.1, 68.2.2, 68.3.0, 68.3.1, 68.4.1, 68.4.2, 68.5.0, 68.6.0, 68.7.0, 68.8.0, 68.8.1, 68.9.0, 68.10.0, 68.11.0, 68.12.0, 68.12.1, 78.0, 78.0.1, 78.1.0, 78.1.1, 78.2.0, 78.2.1, 78.2.2, 78.3.0, 78.3.1, 78.3.2, 78.3.3, 78.4.0, 78.4.1, 78.4.2, 78.4.3, 78.5.0, 78.5.1, 78.6.0, 78.6.1, 78.7.0, 78.7.1, 78.8.0, 78.8.1, 78.9.0, 78.9.1

Рекомендации по устранению

Обновить программное обеспечение

Дата выявления

19 апреля 2021 г.

Дата обновления

19 апреля 2021 г.

Оценка критичности уязвимости (CVSSv3.1)

8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/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://www.cybersecurity-help.cz/vdb/SB2021041920>
<https://www.cybersecurity-help.cz/vdb/SB2021041919>
<https://www.mozilla.org/en-US/security/advisories/mfsa2021-16/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2021-15/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2021-14/>