

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20210129.2 | 29 января 2021 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Множественные уязвимости в Mozilla Firefox

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Mozilla Firefox до v85 Firefox ESR до v78.7
Дата выявления	26 января 2021 г.
Дата обновления	26 января 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-23954	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой смешения типов при использовании операторов логического присваивания.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C</p> <p>CWE-843: Доступ к ресурсам с использованием несовместимых типов (смешение типов)</p> <p>Рекомендации по устранению: обновить программное обеспечение.</p>	8.8

MITRE: CVE-2021-23962	<p>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 HTML-данных.</p> <p>CVSSv3.0: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-119: Выполнение операций за пределами буфера памяти</p> <p>Рекомендации по устранению: обновить программное обеспечение.</p>	7.5
MITRE: CVE-2021-23960 CVE-2021-23964 CVE-2021-23965	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-119: Выполнение операций за пределами буфера памяти</p> <p>Рекомендации по устранению: обновить программное обеспечение.</p>	8.8
Ссылки на источники	<p>https://www.cybersecurity-help.cz/vdb/SB2021012626 https://www.mozilla.org/en-US/security/advisories/mfsa2021-03/ https://www.mozilla.org/en-US/security/advisories/mfsa2021-04/</p>	