

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220511.13 | 11 мая 2022 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Множественные уязвимости в Mozilla Firefox

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Mozilla Firefox: 70.0 - 99.0.1 Firefox ESR: 91.0 - 91.8.0, 78.0 - 78.15.0
Дата выявления	03 мая 2022 г.
Дата обновления	03 мая 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-29909	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной проверкой входных данных.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:U/RL:O/RC:C</p> <p>CWE-264: Некорректное управление генерированием кода (внедрение кода)</p> <p>Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p>	8.1

MITRE: CVE-2022-29917 CVE-2022-29918	<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</p> <p>CWE-119: Выполнение операций за пределами буфера памяти</p> <p>Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p>	8.8
--	---	-----

Ссылки на источники	http://www.mozilla.org/en-US/security/advisories/mfsa2022-16/ http://www.mozilla.org/en-US/security/advisories/mfsa2022-17/	
---------------------	--	--