НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20210714.1 | 14 июля 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Mozilla Firefox

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Mozilla Firefox: 6.0.2, 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, 88.0, 88.0.1, 89.0, 89.0.1, 89.0.2 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, 78.10.0, 78.10.1, 78.11.0
Дата выявления	13 июля 2021 г.
Дата обновления	13 июля 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-29970	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректным использованием памяти в функции специальных возможностей при обработке HTML данных. 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-416: Использование после освобождения Рекомендации по устранению: обновить программное обеспечение.	8.8
MITRE: CVE-2021-29972	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректным использованием памяти в библиотеке Cairo. 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-416: Использование после освобождения Рекомендации по устранению: обновить программное обеспечение.	7.5

MITRE: CVE-2021-29976	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректным определением границ буфера памяти при обработке HTML данных. 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 Рекомендации по устранению: обновить программное обеспечение.	8.8
Ссылки на источники	https://www.mozilla.org/en-US/security/advisories/mfsa2021-28/ https://www.mozilla.org/en-US/security/advisories/mfsa2021-29/ https://www.cybersecurity-help.cz/vdb/SB2021071316	