

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200413.1 | 13 апреля 2020 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Множественные уязвимости в ПО Thunderbird и Firefox

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	Thunderbird до v68.7 firefox (Red Hat package) до v68.6.1-1.el8_1
Дата выявления	9 апреля 2020 г.
Дата обновления	11 апреля 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-6822	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена некорректным условием GMPDecodeData при обработке изображений размером более 4 ГБ в 32-разрядных сборках.</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-787: Запись за границами буфера</p> <p>Рекомендации по устранению: обновить программное обеспечение.</p>	8,8

MITRE:
CVE-2020-6825

Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного веб-сайта. Уязвимость обусловлена ошибкой границ памяти при обработке HTML- страницы.

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/mfsa2020-14/>
<https://www.cybersecurity-help.cz/vdb/SB2020041103>