НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220112.25 | 12 января 2022 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Mozilla Thunderbird и Firefox

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Mozilla Firefox: до 95.0.2 Firefox ESR: до 91.4.1
Дата выявления	11 января 2022 г.
Дата обновления	11 января 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-22742	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти. 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-787: Запись за границами буфера Рекомендации по устранению: обновить программное обеспечение	7.5

MITRE: CVE-2022-22741	Эксплуатация уязвимости позволяет удаленному злоумышленнику блокировать управление целевой системы пользователем посредством отправки специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректным изменением размеров всплывающего окна. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:U/RL:O/RC:C CWE-1021: Некорректное ограничение отображаемых фреймов или слоев интерфейса Рекомендации по устранению: обновить программное обеспечение	7.5
MITRE CVE-2022-22737: CVE-2022-22740	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой использования после освобождения. 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-2022-22738	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти. 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-122: Переполнение буфера в динамической памяти Рекомендации по устранению: обновить программное обеспечение	8.8
MITRE: CVE-2021-4140	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код JavaScript в контексте произвольного окна. Уязвимость обусловлена некорректной реализацией песочницы iframe. 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-254: Уязвимости в безопасности ПО Рекомендации по устранению: обновить программное обеспечение	8.8

MITRE: CVE-2022-22751	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти. 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	http://www.mozilla.org/en-US/security/advisories/mfsa2022-01/ https://www.cybersecurity-help.cz/vdb/SB2022011115 https://www.cybersecurity-help.cz/vdb/SB2022011114 http://www.mozilla.org/en-US/security/advisories/mfsa2022-02/