

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220803.10 | 3 августа 2022 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Выполнение произвольного кода в Mozilla Thunderbird

| | |
|---|--|
| Идентификатор уязвимости | MITRE: CVE-2022-2505 |
| Идентификатор программной ошибки | CWE-119: Выполнение операций за пределами буфера памяти |
| Описание уязвимости | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти. |
| Категория уязвимого продукта | Прикладное программное обеспечение |
| Уязвимый продукт | Mozilla Thunderbird: 102.0 - 102.0.3 |
| 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. |
| Дата выявления | 29 июля 2022 г. |
| Дата обновления | 29 июля 2022 г. |
| Оценка критичности уязвимости (CVSSv3.1) | 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N |
| Вектор атаки (AV) | Сетевой (N) |
| Сложность эксплуатации уязвимости (AC) | Низкая (L) |
| Необходимый уровень привилегий (PR) | Отсутствует (N) |
| Необходимость взаимодействия с пользователем (UI) | Требуется (R) |

| | |
|---|-------------------------|
| Масштаб последствий эксплуатации уязвимости (S) | Не изменяется (U) |
| Влияние на конфиденциальность (C) | Высокое (H) |
| Влияние на целостность (I) | Высокое (H) |
| Влияние на доступность (A) | Высокое (H) |
| Степень зрелости доступных средств эксплуатации | Наличие не подтверждено |
| Наличие средств устранения уязвимости | Официальное решение |
| Достоверность сведений об уязвимости | Сведения подтверждены |

Ссылки на источники

<http://www.mozilla.org/en-US/security/advisories/mfsa2022-32/>