НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20230317.5 | 17 марта 2023 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Mozilla Thunderbird

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Mozilla Thunderbird: 102.1.0 - 102.8.0, 102.5.0 - 102.5.1, 102.4.0 - 102.4.2, 102.3.0 - 102.3.3, 102.0 - 102.0.3
Дата выявления	15 марта 2023 г.
Дата обновления	15 марта 2023 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2023-25751	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной проверкой входных данных. CVSSv3.0: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H CWE-94: Некорректное управление генерированием кода (внедрение кода) 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.	7.5

MITRE: CVE-2023-28176	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 CWE-119: Выполнение операций за пределами буфера памяти 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.	7.5

Ссылки на источники	http://www.mozilla.org/en-US/security/advisories/mfsa2023-11/