НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200706.9| 6 июля 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Mozilla Thunderbird

Идентификатор уязвимости	MITRE: CVE-2020-12419 CVE-2020-12420
Идентификатор программной ошибки	CWE-416: Использование после освобождения
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированной вредоносной веб-страницы. Уязвимость обусловлена некорректным функционированием компонента nsGlobalWindowInner.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	Mozilla Thunderbird: 60.0, 60.2.1, 60.3, 60.3.0, 60.3.1, 60.3.2, 60.3.3, 60.4, 60.4.0, 60.5, 60.5.0, 60.5.1, 60.5.2, 60.5.3, 60.6.0, 60.6.1, 60.7.0, 60.7.1, 60.7.2, 60.8.0, 60.9.0, 60.9.1, 68.0, 68.1.0, 68.1.1, 68.1.2, 68.2.0, 68.2.1, 68.2.2, 68.3.0, 68.3.1, 68.4.1, 68.4.2, 68.5.0, 68.6.0, 68.7.0, 68.8.0, 68.8.1, 68.9.0
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	30 июня 2020 г.
Дата обновления	3 июля 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
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	https://www.cybersecurity-help.cz/vdb/SB2020070301 https://www.mozilla.org/en-US/security/advisories/mfsa2020-26/