НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20190816.1 | 16 августа 2019 г.

Уровень опасности: КРИТИЧЕСКИЙ

Выполнение произвольного кода в Firefox и Thunderbird

Идентификатор уязвимости	MITRE: CVE-2019-11708
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе в результате посещения пользователем вредоносной веб-страницы или открытия электронного письма с вредоносным web-контентом. Уязвимость обусловлена возможностью обхода ограничений безопасности из-за недостаточной проверки параметров в сообщениях Prompt:Open IPC.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	Firefox ESR до v60.7.2 Firefox до v67.0.4 Thunderbird до v60.7.2
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	23 июля 2019 г.
Дата обновления	15 августа 2019 г.
Оценка критичности уязвимости (CVSSv3)	10 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Не требуется (N)
Масштаб последствий эксплуатации уязвимости (S)	Изменяется (C)

Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации (E)	Наличие не подтверждено (U)
Наличие средств устранения уязвимости (RL)	Официальное решение (O)
Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)
Ссылки на источники	https://nvd.nist.gov/vuln/detail/CVE-2019-11708 https://www.mozilla.org/en-US/security/advisories/mfsa2019-20/ https://www.mozilla.org/en-US/security/advisories/mfsa2019-19/