НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20190906.1 | 6 сентября 2019 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение вредоносного кода через параметры командной строки в Mozilla Firefox

Идентификатор уязвимости	MITRE: CVE-2019-9852
Идентификатор программной ошибки	CWE-77: Внедрение команд
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнять произвольные команды в операционных системах семейства Microsoft Windows в результате перехода пользователя из стороннего приложения по специально созданной гиперссылке. Уязвимость обусловлена некорректной очисткой параметров командной строки при запуске Firefox из другого приложения.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	Mozilla Firefox до v68.1
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	3 сентября 2019 г.
Дата обновления	4 сентября 2019 г.
Оценка критичности уязвимости (CVSSv3)	8.8 AV:N/AC:L/PR:N/UI:R/S:U/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)	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 (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://access.redhat.com/security/cve/cve-2019-11751 https://www.mozilla.org/en-US/security/advisories/mfsa2019-26/#CVE-2019-11751