НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200818.7| 18 августа 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Удаленное выполнение команд в Firejail

Идентификатор уязвимости	MITRE: CVE-2020-17367 CVE-2020-17368
Идентификатор программной ошибки	CWE-78:Некорректная нейтрализация специальных элементов, используемых в системных командах (Внедрение команд ОС)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды оболочки в целевой системе посредством отправки специально сформированных данных приложению. Уязвимость обусловлена некорректной проверкой входных данных.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	firejail: 0.9.30, 0.9.32, 0.9.34, 0.9.36, 0.9.38, 0.9.38.2, 0.9.38.4, 0.9.38.8, 0.9.38.10, 0.9.38.12, 0.9.40, 0.9.42, 0.9.44, 0.9.44.2, 0.9.44.4, 0.9.44.6, 0.9.44.8, 0.9.44.10, 0.9.46, 0.9.48, 0.9.50, 0.9.52, 0.9.54, 0.9.56, 0.9.58, 0.9.58.2, 0.9.60, 0.9.62
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	13 августа 2020 г.
Дата обновления	13 августа 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	9.8 AV:N/AC:L/PR:N/UI:N/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)	Не требуется (N)
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://github.com/netblue30/firejail/ https://www.debian.org/security/2020/dsa-4742 https://www.debian.org/security/2020/dsa-4743