НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200602.1 | 2 июня 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольных команд в ClamAV

Идентификатор уязвимости	MITRE: CVE-2020-7613
Идентификатор программной ошибки	CWE-74: Некорректная нейтрализация специальных элементов в выходных данных, отправляемых клиенту (внедрение)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнять произвольные команды в целевой системе. Уязвимость обусловлена некорректной проверкой предоставленных данных в функции _is_clamav_binary в файле Index.js.
Категория уязвимого продукта	Средства защиты информации
Уязвимое ПО	clamscan до v1.2.0
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	7 апреля 2020 г.
Дата обновления	7 апреля 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Высокая (H)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (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://nvd.nist.gov/vuln/detail/CVE-2020-7613 https://snyk.io/vuln/SNYK-JS-CLAMSCAN-564113