

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200513.5 | 13 мая 2020 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **НЕТ**

Возможность инъекции команд ОС в пакете curlrequest для prn

Идентификатор уязвимости	MITRE: CVE-2020-7646
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 использования точки с запятой в любом из значений «параметров». Уязвимость обусловлена некорректной проверкой входных данных.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	curlrequest до v1.0.1
Рекомендации по устранению	На данный момент отсутствуют
Дата выявления	7 мая 2020 г.
Дата обновления	7 мая 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)	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	Концептуальное подтверждение
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2020051309 https://snyk.io/vuln/SNYK-JS-CURLREQUEST-568274