НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200311.1 | 11 марта 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

SQL-инъекция в ПО rConfig

Идентификатор уязвимости	MITRE: CVE-2020-10220
Идентификатор программной ошибки	CWE-89: Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику внедрить вредоносный SQL-код в уязвимое веб-приложение посредством отправки специально созданных SQL-запросов. Уязвимость обусловлена недостаточной фильтрацией параметра searchColumn в файле command.inc.php.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимое ПО	rConfig до v3.9.4
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	7 марта 2020 г.
Дата обновления	9 марта 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	Функциональная версия
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://nvd.nist.gov/vuln/detail/CVE-2020-10220 https://github.com/v1k1ngfr/exploits-rconfig/blob/master/rconfig_sqli.py