

# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: [cert.gov.ru](http://cert.gov.ru)  
E-mail: [threats@cert.gov.ru](mailto:threats@cert.gov.ru)

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200420.2 | 20 апреля 2020 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **НЕТ**

## Выполнение произвольного кода в СУБД SQLite (ONTAP Select Deploy)

Идентификатор уязвимости	MITRE: CVE-2020-11656
Идентификатор программной ошибки	CWE-416: Использование после освобождения
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного вредоносного запроса. Уязвимость обусловлена отсутствием обнуления указателей на освобожденные ячейки памяти при использовании оператора ALTER TABLE.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	SQLite до v3.31.1
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	8 апреля 2020 г.
Дата обновления	16 апреля 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	Наличие не подтверждено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	<a href="https://nvd.nist.gov/vuln/detail/CVE-2020-11656">https://nvd.nist.gov/vuln/detail/CVE-2020-11656</a> <a href="https://security.netapp.com/advisory/ntap-20200416-0001/">https://security.netapp.com/advisory/ntap-20200416-0001/</a>