

# 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-20200618.5 | 18 июня 2020 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **НЕТ**

## Повышение привилегий в targetcli-fb

Идентификатор уязвимости	MITRE: CVE-2020-13867
Идентификатор программной ошибки	CWE-276: Некорректные разрешения, назначаемые по умолчанию
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику повысить свои привилегии в целевой системе. Уязвимость обусловлена некорректным разграничением прав доступа для конфигурационных файлов в директории /etc/target.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	targetcli-fb 2.1.50, 2.1.51, 2.1.52
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	5 июня 2020 г.
Дата обновления	11 июня 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	Недоступно
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	<a href="https://www.cybersecurity-help.cz/vdb/SB2020061608">https://www.cybersecurity-help.cz/vdb/SB2020061608</a> <a href="https://github.com/open-iscsi/targetcli-fb/pull/172">https://github.com/open-iscsi/targetcli-fb/pull/172</a>