

# 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-20200330.2 | 30 марта 2020 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

## Повышение привилегий в HashiCorp Vault и Vault Enterprise

Идентификатор уязвимости	MITRE: CVE-2020-10661
Идентификатор программной ошибки	CWE-264: Уязвимость в управлении доступом, привилегиями и разрешениями
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику повысить свои привилегии в целевой системе. Уязвимость обусловлена некорректной обработкой политикой безопасности вложенных правил.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	HashiCorp Vault версий 0.11.0 - 0.11.6, 1.0.0 - 1.0.3, 1.1.0 - 1.1.5, 1.2.0 - 1.2.4 и 1.3.0 - 1.3.3 HashiCorp Vault Enterprise версий 0.11.0 - 0.11.6, 1.0.0 - 1.0.3, 1.1.0 - 1.1.5, 1.2.0 - 1.2.4 и 1.3.0 - 1.3.3
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	19 марта 2020 г.
Дата обновления	30 марта 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
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)

Отсутствует (N)

Степень зрелости доступных средств эксплуатации

Наличие не подтверждено

Наличие средств устранения уязвимости

Официальное решение

Достоверность сведений об уязвимости

Сведения подтверждены

---

Ссылки на источники

<https://github.com/hashicorp/vault/blob/master/CHANGELOG.md#134-march-19th-2020>  
<https://github.com/hashicorp/vault/commit/18485ee9d4352ac8e8396c580b5941ccf8e5b31a>  
<https://www.cybersecurity-help.cz/vdb/SB2020033005>