

# 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-20200326.2 | 26 марта 2020 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

## Удаленное выполнение произвольного кода в ОС CentOS

Идентификатор уязвимости	MITRE: CVE-2020-5312
Идентификатор программной ошибки	CWE-119: Выполнение операций за пределами буфера памяти
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена ошибкой границ памяти в файле libImaging / PcxDecode.c при обработке изображений PCX.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимое ПО	CentOS: 6
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	26 марта 2020 г.
Дата обновления	26 марта 2020 г.
Оценка критичности уязвимости (CVSSv3.0)	8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Требуется (R)
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

<https://www.cybersecurity-help.cz/vdb/SB2020032601>