

# 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-20210219.4 | 19 февраля 2021 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

## Выполнение произвольного кода в Cisco AnyConnect Secure Mobility Client для Windows

Идентификатор уязвимости	MITRE: CVE-2021-1366
Идентификатор программной ошибки	CWE-347: Некорректная проверка криптографической подписи
Описание уязвимости	Эксплуатация уязвимости позволяет аутентифицированному локальному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного IPC-сообщения процессу AnyConnect. Уязвимость обусловлена некорректной проверкой пути расположения DLL библиотек при загрузке уязвимого приложения с модулем VPN Posture.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Cisco AnyConnect Secure Mobility Client для Windows до v4.9.05042
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	17 февраля 2021 г.
Дата обновления	17 февраля 2021 г.
Оценка критичности уязвимости (CVSSv3.0)	7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Локальный (L)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Низкий (L)
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

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-dll-hijac-lrcTOQMC>