

# 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-20211115.2 | 15 ноября 2021 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

## НСД к данным в RoboHelp Server

Идентификатор уязвимости	MITRE: CVE-2021-42727
Идентификатор программной ошибки	CWE-22: Некорректные ограничения путей для каталогов (выход за пределы каталога)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к файлам и директориям в целевой системе посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных данных.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	RoboHelp Server: 2020.0, 2020.0.1
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	12 ноября 2021 г.
Дата обновления	12 ноября 2021 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://www.cybersecurity-help.cz/vdb/SB2021111212">https://www.cybersecurity-help.cz/vdb/SB2021111212</a> <a href="http://helpx.adobe.com/security/products/robohelp-server/apsb21-87.html">http://helpx.adobe.com/security/products/robohelp-server/apsb21-87.html</a>