

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220112.1 | 12 января 2022 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

Чтение произвольных файлов в Sphinx

Идентификатор уязвимости	MITRE: CVE-2020-29050
Идентификатор программной ошибки	CWE-22: Некорректные ограничения путей для каталогов (выход за пределы каталога)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику прочитать произвольный файлы в целевой системе посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных данных при обработке последовательностей обхода каталогов.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	Sphinx: до 3.1.1
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	11 января 2022 г.
Дата обновления	11 января 2022 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://www.cybersecurity-help.cz/vdb/SB2022011110>
<http://security-tracker.debian.org/tracker/CVE-2020-29050>
<http://blog.wirhabenstil.de/2019/08/19/sphinxsearch-0-0-0-09306-cve-2019-14511/>