

# 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-20211112.4 | 12 ноября 2021 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

## Выполнение произвольного кода в Palo Alto PAN-OS

Идентификатор уязвимости	MITRE: CVE-2021-3064
Идентификатор программной ошибки	CWE-119: Выполнение операций за пределами буфера памяти
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена ошибкой границ памяти в конфигурациях брандмауэра PAN-OS с включенным порталом GlobalProtect или шлюзом.
Категория уязвимого продукта	UNIX-подобные операционные системы
Уязвимый продукт	Palo Alto PAN-OS: 8.1, 8.1.0, 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.1.4-h2, 8.1.5, 8.1.6, 8.1.6-h2, 8.1.7, 8.1.8, 8.1.8-h4, 8.1.8-h5, 8.1.9, 8.1.9-h4, 8.1.10, 8.1.11, 8.1.12, 8.1.13, 8.1.14, 8.1.14-h2, 8.1.15, 8.1.15-h3, 8.1.16
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	11 ноября 2021 г.
Дата обновления	11 ноября 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	10.0 AV:N/AC:L/PR:N/UI:N/S:C/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)	Изменяется (C)
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/SB2021111106>  
<http://security.paloaltonetworks.com/CVE-2021-3064>  
<http://www.randori.com/blog/cve-2021-3064/>