НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20201231.1 | 31 декабря 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Повышение привилегий в Palo Alto PAN-OS

Идентификатор уязвимости	MITRE: CVE-2020-2000
Идентификатор программной ошибки	CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику повысить свои привилегии и выполнить произвольные команды в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных в веб-интерфейсе управления PAN-OS.
Категория уязвимого продукта	Телекоммуникационное оборудование
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, 8.1.15, 9.0, 9.0.0, 9.0.1, 9.0.2, 9.0.2-h4, 9.0.3, 9.0.3-h2, 9.0.3-h3, 9.0.4, 9.0.5, 9.0.5-h3, 9.0.6, 9.0.7, 9.0.8, 9.0.9, 9.1, 9.1.0, 9.1.1, 9.1.2, 9.1.3, 9.2.0, 10.0
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	12 ноября 2020 г.
Дата обновления	12 ноября 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	7.2 AV:N/AC:L/PR:H/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)	Высокий (H)

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://www.cybersecurity-help.cz/vdb/SB2020111220 https://security.paloaltonetworks.com/CVE-2020-2000