НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20190828.4 | 28 августа 2019 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Удаленное выполнение кода в ОС PAN-OS

Идентификатор уязвимости	MITRE: CVE-2019-1581
Идентификатор ошибки	CWE-20: Некорректная проверка ввода
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код на целевом устройстве посредством отправки специально сформированного сетевого пакета. Уязвимость обусловлена некорректной проверкой предоставленных данных.
Категория уязвимого продукта	Средства защиты информации
Уязвимое ПО	PAN-OS до v9.0.3.
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	22 августа 2019 г.
Дата обновления	24 августа 2019 г.
Оценка критичности уязвимости (CVSSv3)	9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Не требуется (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 (E)	Наличие не подтверждено (U)
Наличие средств устранения уязвимости (RL)	Официальное решение (O)
Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)
Ссылки на источники	https://nvd.nist.gov/vuln/detail/CVE-2019-1581 https://securityadvisories.paloaltonetworks.com/Home/Detail/160