НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200914.1 | 14 сентября 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в PAN-OS

Категория уязвимого продукта	Unix-подобные операционные системы и их компоненты
Уязвимый продукт	PAN-OS до следующих версий: v8.1.15, v9.0.9, v9.1.3
Дата выявления	10 сентября 2020 г.
Дата обновления	10 сентября 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-2040	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код с привилегиями root в целевой системе посредством отправки вредоносного запроса в интерфейс аутентификации. Уязвимость обусловлена ошибкой границ памяти при обработке запросов в сетевом сервисе Captive Portal или интерфейсе многофакторной аутентификации. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-119: Выполнение операций за пределами буфера памяти Рекомендации по устранению: обновить программное обеспечение.	10.0

MITRE: CVE-2020-2036	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить отраженный межсайтовый скриптинг посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной очисткой предоставленных пользователем данных в веб-интерфейсе управления PAN-OS. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-79: Некорректная нейтрализация входных данных при генерировании веб-страниц (межсайтовое выполнение сценариев) Рекомендации по устранению: обновить программное обеспечение.	8.8
Ссылки на источники	https://security.paloaltonetworks.com/CVE-2020-2036 https://www.cybersecurity-help.cz/vdb/SB2020091017 https://security.paloaltonetworks.com/CVE-2020-2040 https://www.cybersecurity-help.cz/vdb/SB2020091012	