НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20230321.3 | 21 марта 2023 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Aruba ClearPass Policy Manager

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	ClearPass Policy Manager: 6.9.0 - 6.11.1
Дата выявления	15 марта 2023 г.
Дата обновления	15 марта 2023 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2023-25589	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена некорректными ограничениями доступа к веб-интерфейсу управления. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H CWE-284: Некорректное управление доступом Рекомендации по устранению: данная уязвимость устраняется официальным патчем вендора. в связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	9.8

MITRE: CVE-2023-25590	Эксплуатация уязвимости позволяет аутентифицированному локальному злоумышленнику повысить свои привилегии в целевой системе. Уязвимость обусловлена некорректными ограничениями безопасности в агенте ClearPass OnGuard Linux. CVSSv3.0: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H CWE-264: Уязвимость в управлении доступом, привилегиями и разрешениями Рекомендации по устранению: данная уязвимость устраняется официальным патчем вендора. в связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	7.8
MITRE: CVE-2023-25591	Эксплуатация уязвимости позволяет аутентифицированному удаленному злоумышленнику НСД к целевой системе. Уязвимость обусловлена некорректным выводом данных приложением в веб-интерфейс управления. CVSSv3.0: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L CWE-200: Разглашение важной информации лицам без соответствующих прав Рекомендации по устранению: данная уязвимость устраняется официальным патчем вендора. в связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	7.6
MITRE: CVE-2023-25592 CVE-2023-25593	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнять атаки с использованием межсайтовых сценариев посредством открытия пользователем специально созданной вредоносной ссылки. Уязвимость обусловлена CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L CWE-79: Некорректная нейтрализация входных данных при генерировании веб-страниц (межсайтовое выполнение сценариев) Рекомендации по устранению: данная уязвимость устраняется официальным патчем вендора. в связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	7.1

Ссылки на источники	http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt