

# 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-20200720.1 | 20 июля 2020 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

## Удаленное выполнение кода в маршрутизаторах серий Moxa EDR-G902 и EDR-G903

Идентификатор уязвимости	MITRE: CVE-2020-14511
Идентификатор программной ошибки	CWE-121: Переполнение буфера в стеке
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством выполнения вредоносных операций со специально сформированными куки-файлами веб-браузера. Уязвимость обусловлена некорректной обработкой куки-файлов на веб-сервере уязвимого оборудования.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	EDR-G902 и EDR-G903 с версией ПО 5.4 или ниже
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	15 июня 2020 г.
Дата обновления	17 июля 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
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)	Не изменяется (U)
Влияние на конфиденциальность (C)	Отсутствует (N)
Влияние на целостность (I)	Отсутствует (N)

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.moxa.com/en/support/support/security-advisory/edr-g902-g903-series-secure-routers-vulnerabilities>

<https://us-cert.cisa.gov/ics/advisories/icsa-20-196-02>