НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200810.10 | 10 августа 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Moxa MGate 5105-MB-EIP Series

Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	MGate 5105-MB-EIP: -, 4.2
Дата выявления	10 июля 2020 г.
Дата обновления	31 июля 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-15494	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить идентификатор сеанса соединения между хостом и целевым устройством. Уязвимость обусловлена некорректной процедурой аутентификации на уязвимом устройстве. CVSSv3.1: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C CWE-294: Обход аутентификации при помощи перехвата и воспроизведения Рекомендации по устранению: обновить программное обеспечение.	7.5

MITRE: CVE-2020-15493	Эксплуатация уязвимости позволяет удаленному злоумышленнику расшифровать зашифрованный файл конфигурации устройства. Уязвимость обусловлена некорректной проверкой входных данных. CVSSv3.1: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C CWE-200: Разглашение конфиденциальной информации неавторизованному субъекту Рекомендации по устранению: обновить программное обеспечение.	7.5

Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2020071010 https://www.moxa.com/en/support/support/security-advisory/mgate-5105-mb-eip-series-protocol-gateways-vulnerabilities https://reportcybercrime.com/multiple-vulnerabilities-in-moxa-mgate-5105-mb-eip-series/