НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200317.1 | 17 марта 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Удаленное выполнение кода в ПО OnCell Central Manager компании Moxa

Идентификатор уязвимости	MITRE: CVE-2019-15696
Идентификатор программной ошибки	CWE-502: Десериализация недоверенных данных
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных сетевых пакетов. Уязвимость обусловлена некорректной работой встроенного компонента Apache Flex BlazeDS.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимое ПО	Moxa OnCell Central Manager до v2.4.1
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	16 марта 2020 г.
Дата обновления	16 марта 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	8.5 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
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)	Высокое (H)
Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Высокое (H)

Степень зрелости доступных средств эксплуатации	Концептуальное подтверждение
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://www.moxa.com/en/support/support/security-advisory/oncell-central-manager-cellular-management-software-vulnerabilities https://ics-cert.kaspersky.com/advisories/klcert-advisories/2020/03/16/klcert-20-001-remote-code-execution-on-moxas-cellular-management-software-oncell-central-manager-version-lower-than-2-4-1/ https://www.cybersecurity-help.cz/vdb/SB2020031603