

# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20201112.1 | 12 ноября 2020 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

## Повышение привилегий в Моха MXView

Идентификатор уязвимости	MITRE: CVE-2020-13536 CVE-2020-13537
Идентификатор программной ошибки	CWE-276: Некорректные разрешения, назначаемые по умолчанию
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды с привилегиями пользователя «NT SYSTEM» в целевой системе посредством изменения файла, который выполняется при запуске системы. Уязвимость обусловлена некорректными разрешениями в файловой системе.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Моха MXView Series 3.1.8
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	5 ноября 2020 г.
Дата обновления	6 ноября 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	9.3 AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
Вектор атаки (AV)	Локальный (L)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)
Масштаб последствий эксплуатации уязвимости (S)	Изменяется (C)
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://talosintelligence.com/vulnerability\\_reports/TALOS-2020-1148](https://talosintelligence.com/vulnerability_reports/TALOS-2020-1148)