НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210910.5 | 10 сентября 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Повышение привилегий в Cisco IOS XR

Идентификатор уязвимости	MITRE: CVE-2021-34719 CVE-2021-34728
Идентификатор программной ошибки	CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)
Описание уязвимости	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе посредством ввода специально сформированной вредоносной команды. Уязвимость обусловлена некорректной проверкой ввода в интерфейсе командной строки программного обеспечения Cisco IOS XR.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco IOS XR: 6.8, 7.0, 7.0.1, 7.0.2, 7.0.14, 7.0.90, 7.1, 7.1.1, 7.1.2, 7.1.3, 7.1.15, 7.1.25, 7.2.0, 7.2.1, 7.2.2, 7.2.12, 7.3, 7.3.0, 7.3.1, 7.3.15, 7.4
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	9 сентября 2021 г.
Дата обновления	9 сентября 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Локальный (L)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Низкий (L)
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	Наличие не подтверждено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2021090915 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-privescal-dZYMrKf