НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20211008.4 | 8 октября 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольных команд в Cisco Intersight Virtual Appliance

Идентификатор уязвимости	MITRE: CVE-2021-34748
Идентификатор программной ошибки	CWE-77: Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольные команды в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных в веб-интерфейсе управления.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco Intersight Virtual Appliance: 1.0.9 292, 1.0.9-150
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	7 октября 2021 г.
Дата обновления	7 октября 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:N/AC:L/PR:L/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)	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/SB2021100702 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsi2-command-inject-CGyC8y2R