НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20211008.1 | 8 октября 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольных команд в Cisco Identity Services Engine

Идентификатор уязвимости	MITRE: CVE-2021-1594
Идентификатор программной ошибки	CWE-266: Некорректное назначение привилегий
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды с привилегиями пользователя root в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных для конечных точек API.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco Identity Services Engine: 2.4, 2.6, 2.7, 3.0
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	7 октября 2021 г.
Дата обновления	7 октября 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	7.5 AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Высокая (H)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Требуется (R)
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/SB2021100707 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-priv-esc-UwqPrBM3