НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220125.8 | 25 января 2022 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Повышение привилегий в Cisco Unified Contact Center Management Portal

Идентификатор уязвимости	MITRE: CVE-2022-20658
Идентификатор программной ошибки	CWE-602: Обеспечение безопасности сервера на стороне клиента
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена некорректной проверкой пользовательских разрешений.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Unified Contact Center Management Portal: до 11.6.1, 12.0.1, 12.5.1
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	24 января 2022 г.
Дата обновления	24 января 2022 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/SB2022012421 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ccmp-priv-esc-JzhTFLm4 http://bst.cloudapps.cisco.com/bugsearch/bug/CSCvz49473