НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20221116.4 | 16 ноября 2022 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в Zoom Client for macOS

Идентификатор уязвимости	MITRE: CVE-2022-28768
Идентификатор программной ошибки	CWE-276: Некорректные разрешения, назначаемые по умолчанию
Описание уязвимости	Эксплуатация уязвимости позволяет аутентифицированному локальному злоумышленнику выполнить произвольный код с привилегиями «root» в целевой системе. Уязвимость обусловлена некорректными разрешениями по умолчанию в установщике Zoom Rooms для macOS.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Zoom Client for macOS: 5.0.0 23186.0427 - 5.12.3 11845
Рекомендации по устранению	Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.
Дата выявления	16 ноября 2022 г.
Дата обновления	16 ноября 2022 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 CVSS:3.1/AV:L/AC:L/PR:L/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)	Низкий (L)
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	Не определено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Не определено
Ссылки на источники	http://explore.zoom.us/en/trust/security/security-bulletin/#ZSB-22029