НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220822.21 | 22 августа 2022 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Повышение привилегий в Zoom Rooms for Windows

Идентификатор уязвимости	MITRE: CVE-2022-28752
Идентификатор программной ошибки	CWE-59: Некорректное разрешение ссылки перед доступом к файлу ("переход по ссылке")
Описание уязвимости	Эксплуатация уязвимости позволяет аутентифицированному локальному злоумышленнику повысить свои привилегии в целевой системе. Уязвимость обусловлена некорректным разрешением ссылки для доступа к критически важному файлу.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Zoom Rooms for Windows: 4.6.5 18374.0407 - 5.10.6 1421
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	18 августа 2022 г.
Дата обновления	18 августа 2022 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 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	Наличие не подтверждено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	http://explore.zoom.us/en/trust/security/security-bulletin/#ZSB-22013