НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20221116.3 | 16 ноября 2022 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в Zoom Client for Windows

Идентификатор уязвимости	MITRE: CVE-2022-28766
Идентификатор программной ошибки	CWE-427: Неконтролируемый элемент пути поиска
Описание уязвимости	Эксплуатация уязвимости позволяет аутентифицированному локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного DLL-файла. Уязвимость обусловлена небезопасной загрузкой библиотеки DLL.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Zoom Client for Windows: 5.0.0 23168.0427 - 5.12.3 9638 Virtual Desktop Infrastructure (VDI): 5.0.1 - 5.12.3 Zoom Rooms for Windows: 5.0.0 1420.0426 - 5.12.2 1970
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)	8.1 CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:L
Вектор атаки (AV)	Локальный (L)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Низкий (L)
Необходимость взаимодействия с	Требуется (R)

пользователем (UI)	
Масштаб последствий эксплуатации уязвимости (S)	Изменяется (C)
Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Низкое (L)
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-22027