НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210322.7 | 22 марта 2021 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в Adobe Connect

Идентификатор уязвимости	MITRE: CVE-2021-21085
Идентификатор программной ошибки	CWE-20: Некорректная проверка входных данных
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной проверкой входных данных.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Adobe Connect:8.0, 8.2.1, 8.2.1.3, 8.2.2, 8.2.2.2, 9.0, 9.0.1, 9.0.2, 9.0.3, 9.0.4, 9.1, 9.1.1, 9.1.2, 9.2, 9.2.1, 9.2.2, 9.3, 9.4, 9.4.1, 9.4.2, 9.5, 9.5.1, 9.5.2, 9.5.3, 9.5.4, 9.5.5, 9.5.6, 9.5.7, 9.6, 9.6.1, 9.6.2, 9.7, 9.7.5, 9.8, 9.8.1, 10.0, 10.1, 10.2, 10.5, 10.6, 10.6.1, 10.6.2, 10.8, 11.0, 11.0.5
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	9 марта 2021 г.
Дата обновления	9 марта 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	9.8 AV:N/AC:L/PR:N/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)	Отсутствует (N)
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/SB2021031001 https://helpx.adobe.com/security/products/connect/apsb21-19.html