

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200319.7 | 19 марта 2020 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

PHP-инъекция в Adobe ColdFusion

Идентификатор уязвимости	MITRE: CVE-2020-3794
Идентификатор программной ошибки	CWE-98: Уязвимости, связанные с именами файлов для PHP-функций include или require
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный PHP код в целевой системе посредством отправки специально сформированного HTTP запроса
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	Adobe ColdFusion 2016 Update 13 и ниже Adobe ColdFusion 2018 Update 7 и ниже
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	20 февраля 2020 г.
Дата обновления	2 марта 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	8.5 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://helpx.adobe.com/security/products/coldfusion/apsb20-16.html>