

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200319.8 | 19 марта 2020 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Множественные уязвимости в Adobe Bridge

Идентификатор уязвимости	MITRE: CVE-2020-9551 CVE-2020-9552
Идентификатор программной ошибки	CWE-787: Запись за границами буфера CWE-122: Переполнение буфера в динамической памяти
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством переполнения буфера или записи за его границу.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	Adobe Bridge CC версии 10.0
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	17 марта 2020 г.
Дата обновления	18 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/bridge/apsb20-17.html>