

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20210917.19 | 17 сентября 2021 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Выполнение произвольного кода в Adobe InDesign

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Adobe InDesign: 16.0, 16.0.1, 16.0.2, 16.1, 16.2, 16.2.1, 16.3, 16.3.1, 16.3.2
Дата выявления	16 сентября 2021 г.
Дата обновления	16 сентября 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-39820	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C</p> <p>CWE-119: Выполнение операций за пределами буфера памяти</p> <p>Рекомендации по устранению: обновить программное обеспечение</p>	8.8

MITRE: CVE-2021-39821 CVE-2021-39822	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена некорректной обработкой входящих данных.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C</p> <p>CWE-125: Чтение за пределами буфера</p> <p>Рекомендации по устранению: обновить программное обеспечение</p>	8.8
--	--	-----

Ссылки на источники	<p>https://www.cybersecurity-help.cz/vdb/SB2021091609</p> <p>https://helpx.adobe.com/security/products/indesign/apsb21-73.html</p>
---------------------	---