НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210322.9 | 22 марта 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в Microsoft PowerPoint

Идентификатор уязвимости	MITRE: CVE-2021-27056
Идентификатор программной ошибки	CWE-94: Некорректное управление генерированием кода (внедрение кода)
Описание уязвимости	Эксплуатация уязвимости позволяет злоумышленнику выполнить произвольный код в целевой системе посредством открытия вредоносной страницы или вредоносного файла презентации. Уязвимость обусловлена некорректной проверкой существования объекта перед выполнением операций с ним при обработке файлов презентаций.
Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
Уязвимый продукт	Microsoft Office: 2019 Microsoft PowerPoint: 2010 Service Pack 2, 2013 RT Service Pack 1, 2013 Service Pack 1, 2016
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	9 марта 2021 г.
Дата обновления	9 марта 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Локальный (L)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Требуется (R)
Масштаб последствий эксплуатации	Не изменяется (U)

уязвимости (S)	
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/SB2021030935 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27056