НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20201015.2 | 15 октября 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Удаленное выполнение кода в Microsoft Office Access Connectivity Engine

Идентификатор уязвимости	MITRE: CVE-2020-16957
Идентификатор программной ошибки	CWE-119: Выполнение операций за пределами буфера памяти
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного вредоносного файла. Уязвимость обусловлена некорректным определением границ буфера памяти при функционировании уязвимого ПО.
Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
Уязвимый продукт	Microsoft Office: 2019 Microsoft 365 Apps for Enterprise: 32-bit Systems, 64-bit Systems
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	13 октября 2020 г.
Дата обновления	14 октября 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:N/AC:L/PR:N/UI:R/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)	Требуется (R)

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/SB2020101368 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16957