НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220602.6 | 2 июня 2022 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: НЕТ

Выполнение произвольного кода в Microsoft Office

Идентификатор уязвимости	Не определен
Идентификатор программной ошибки	Не определен
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного DOC-файла. Уязвимость обусловлена возможностью запуска настраиваемого поиска. При открытии вредоносного DOC-файла происходит подключение к удаленному сетевому хранилищу при помощи URI-протокола “search-ms“, откуда в последующем будет загружена полезная нагрузка, позволяющая выполнять произвольный код в системе.
Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
Уязвимый продукт	Microsoft Word: 2016 - 2021 Microsoft Office: 2016 - 2021
Рекомендации по устранению	Рекомендуем не скачивать и не открывать DOC-файлы из не доверенных источников.
Дата выявления	02 июня 2022 г.
Дата обновления	02 июня 2022 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с	Требуется (R)

пользователем (UI)	
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	Недоступно
Достоверность сведений об уязвимости	Сведения подтверждены

Ссылки на источники