НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20230315.2 | 15 марта 2023 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Компрометация учетной записи в Microsoft Outlook

Идентификатор уязвимости	MITRE: CVE-2023-23397
Идентификатор программной ошибки	CWE-200: Разглашение важной информации лицам без соответствующих прав
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить хэш Net-NTLMv2 и с помощью него скомпрометировать уязвимую систему посредством отправки специально созданного вредоносного сообщения. Уязвимость обусловлена утечкой в приложение хэша Net-NTLMv2.
Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
Уязвимый продукт	Microsoft Outlook: 2013 - 2021 Microsoft Office: 365 - 2021
Рекомендации по устранению	Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.
Дата выявления	14 марта 2023 г.
Дата обновления	14 марта 2023 г.
Оценка критичности уязвимости (CVSSv3.1)	9.8 CVSS:3.1/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	Отсутствует (N)

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	Функциональная версия (F)
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Не определено
Ссылки на источники	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-23397