НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20230215.5 | 15 февраля 2023 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в Microsoft Exchange Server

Идентификатор уязвимости	MITRE: CVE-2023-21706
Идентификатор программной ошибки	CWE-94: Некорректное управление генерированием кода (внедрение кода)
Описание уязвимости	Эксплуатация уязвимости позволяет аутентифицированному удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной проверкой входных данных.
Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
Уязвимый продукт	Microsoft Exchange Server: 2019 Preview 15.02.0196.000 - 2019 CU12 Feb23SU 15.02.1118.025, 2013 RTM 15.00.0516.032 - 2013 CU23 Feb23SU 15.00.1497.047, 2019 CU12 Jan23SU 15.02.1118.021, 2019 CU12 Oct22SU 15.02.1118.015, 2019 CU11 Oct22SU 15.02.0986.030, 2019 CU11 Nov22SU 15.02.0986.036, 2019 CU12 Nov22SU 15.02.1118.020, 2016 CU23 Jan23SU 15.01.2507.017, 2016 CU22 Oct22SU 15.01.2375.032, 2016 CU23 Oct22SU 15.01.2507.013, 2016 CU22 Nov22SU 15.01.2375.037, 2016 CU23 Nov22SU 15.01.2507.016, 2016 Preview 15.01.0225.016 - 2016 CU23 Feb23SU 15.01.2507.021, 2013 CU23 Jan23SU 15.00.1497.045, 2013 CU23 Oct22SU 15.00.1497.042, 2013 CU23 Nov22SU 15.00.1497.044
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 февраля 2023 г.
Дата обновления	14 февраля 2023 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 CVSS:3.1/AV:N/AC:L/PR:L/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)	Низкий (L)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)
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	Не определено
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-2023-21706