НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20230321.2 | 21 марта 2023 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в Microsoft Internet Control Message Protocol (ICMP)

Идентификатор уязвимости	MITRE: CVE-2023-23415
Идентификатор программной ошибки	CWE-20: Некорректная проверка входных данных
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных.
Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
Уязвимый продукт	Windows: 10 - 11 22H2 Windows Server: 2008 - 2022
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 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://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23415