НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20230125.7 | 25 января 2023 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Microsoft Exchange Server

Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
Уязвимый продукт	Microsoft Exchange Server: 2019 Preview 15.02.0196.000 - 2019 Cumulative Update 12 Aug22SU 15.02.1118.012, 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 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 Cumulative Update 23 Aug22SU 15.01.2507.012, 2016 CU23 Jan23SU 15.01.2507.017, 2019 CU12 Jan23SU 15.02.1118.021
Дата выявления	10 января 2023 г.
Дата обновления	10 января 2023 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2023-21745 CVE-2023-21762	Эксплуатация уязвимости позволяет локальному злоумышленнику провести спуфинг атаку на целевую систему. CVSSv3.0: AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.0

	CWE-300: Возможность доступа к каналу из точки, не являющейся конечной (человек посередине) 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.	
MITRE: CVE-2023-21761	Эксплуатация уязвимости позволяет аутентифицированному удаленному злоумышленнику получить НСД к данным посредством запуска специально созданного вредоносного файла. Уязвимость обусловлена некорректной работой криптографического компонента. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N CWE-200: Разглашение важной информации лицам без соответствующих прав 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.	7.5
MITRE: CVE-2023-21763 CVE-2023-21764	Эксплуатация уязвимости позволяет аутентифицированному локальному злоумышленнику повысить свои привилегии в целевой системе посредством запуска специально созданного вредоносного файла. CVSSv3.0: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H CWE-264: Уязвимость в управлении доступом, привилегиями и разрешениями 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.	7.8

Ссылки на источники	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21745 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21764 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21762 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21761 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21763