НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20221116.8 | 16 ноября 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Microsoft Edge

Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
Уязвимый продукт	Microsoft Edge: 79.0.309.71 - 107.0.1418.35
Дата выявления	11 ноября 2022 г.
Дата обновления	11 ноября 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-3885 CVE-2022-3886 CVE-2022-3887 CVE-2022-3888	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой использования после освобождения. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H CWE-416: Использование после освобождения 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.	8.8

MITRE: CVE-2022-3889	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой смешения типов. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H CWE-843: Доступ к ресурсам с использованием несовместимых типов (смешение типов) 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.	8.8
MITRE: CVE-2022-3890	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H CWE-122: Переполнение буфера в динамической памяти 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.	9.6

Ссылки на источники	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3889 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3890 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3888 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3885 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3886 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3887