НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20230331.3 | 31 марта 2023 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 - 111.0.1661.51
Дата выявления	25 марта 2023 г.
Дата обновления	25 марта 2023 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2023-1528 CVE-2023-1530 CVE-2023-1531 CVE-2023-1533	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-2023-1529	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:N/S:U/C:H/I:H/A:H CWE-119: Выполнение операций за пределами буфера 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.	9.8
MITRE: CVE-2023-1532 CVE-2023-1534	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить конфиденциальную информацию из целевой системы посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена граничным состоянием в компоненте GPU Video. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H CWE-125: Чтение за пределами буфера 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

Ссылки на источники	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-1528 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-1531 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-1532 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-1534 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-1529 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-1533 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-1530