# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220727.14 | 27 июля 2022 г.

Уровень опасности: ВЫСОКИЙ

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 - 103.0.1264.62 |
| Дата выявления | 23 июля 2022 г. |
| Дата обновления | 23 июля 2022 г. |

| Идентификатор уязвимости | Описание уязвимости | Базовый уровень CVSS |
|---|---|---|
| MITRE:<br>CVE-2022-2477<br>CVE-2022-2478<br>CVE-2022-2480<br>CVE-2022-2481 | 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.<br><br>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C<br><br>CWE-416: Использование после освобождения<br><br>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:<br>CVE-2022-2479 | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной проверкой входных данных.<br><br>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C<br><br>CWE-20: Некорректная проверка входных данных<br><br>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-2022-2479<br>http://crbug.com/1335861<br>http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-2478<br>http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-2481<br>http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-2477<br>http://chromereleases.googleblog.com/2022/07/stable-channel-update-for-desktop_19.html<br>http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-2480<br>http://crbug.com/1341603<br>http://crbug.com/1336266<br>http://crbug.com/1339844<br>http://crbug.com/1329987 |