# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20211217.10 | 17 декабря 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

## Множественные уязвимости в Microsoft Edge (Chromium-based)

| | |
|---|---|
| Категория уязвимого продукта | Прикладное программное обеспечение |
| Уязвимый продукт | Microsoft Edge (Chromium-based): до 96.0.1054.43 |
| Дата выявления | 6 декабря 2021 г. |
| Дата обновления | 10 декабря 2021 г. |

| Идентификатор уязвимости | Описание уязвимости | Базовый уровень CVSS |
|---|---|---|
| MITRE:<br>CVE-2021-4055<br>CVE-2021-4058<br>CVE-2021-4062 | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти.<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>CWE-122: Переполнение буфера в динамической памяти<br>Рекомендации по устранению: обновить программное обеспечение | 8.8 |

| | | |
|---|---|---|
| MITRE:<br>CVE-2021-4052<br>CVE-2021-4053<br>CVE-2021-4057<br>CVE-2021-4063<br>CVE-2021-4064<br>CVE-2021-4065<br>CVE-2021-4067 | 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>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>CWE-416: Использование после освобождения<br>Рекомендации по устранению: обновить программное обеспечение | 8.8 |
| MITRE:<br>CVE-2021-4066 | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена целочисленным переполнения.<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>CWE-191: Потеря значимости целых чисел (простой или циклический возврат)<br>Рекомендации по устранению: обновить программное обеспечение | 8.8 |
| MITRE:<br>CVE-2021-4056<br>CVE-2021-4061 | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой смешения типов.<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>CWE-843: Доступ к ресурсам с использованием несовместимых типов (смешение типов)<br>Рекомендации по устранению: обновить программное обеспечение | 8.8 |

| | | |
|---|---|---|
| MITRE: CVE-2021-4059 | 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>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C<br>CWE-20: Некорректная проверка входных данных<br>Рекомендации по устранению: обновить программное обеспечение | 7.5 |
| MITRE: CVE-2021-4054 | Эксплуатация уязвимости позволяет удаленному злоумышленнику НДС к целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной проверкой входных данных.<br>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:U/RL:O/RC:C<br>CWE-451: Некорректное представление важной информации интерфейсом пользователя<br>Рекомендации по устранению: обновить программное обеспечение | 8.1 |

| | |
|---|---|
| Ссылки на источники | https://www.cybersecurity-help.cz/vdb/SB2021121016<br>http://chromereleases.googleblog.com/2021/12/stable-channel-update-for-desktop.html<br>http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4053<br>http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4056<br>http://crbug.com/1239760<br>http://crbug.com/1273674<br>http://crbug.com/1273176<br>http://crbug.com/1274641<br>http://crbug.com/1271456<br>http://crbug.com/1272403<br>http://crbug.com/1260939<br>http://crbug.com/1267661<br>http://crbug.com/1270990<br>http://crbug.com/1267496<br>http://crbug.com/1262183 |

http://crbug.com/1273197
http://crbug.com/1266510
http://crbug.com/1274499
http://crbug.com/1267791
http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4066
http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4065
http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4052
http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4063
http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4054
http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4058
http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4067
http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4062
http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4061
http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4059
http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4064
http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4057
http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4055