# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20210818.1 | 18 августа 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

## Множественные уязвимости в Google Chrome

| | |
|---|---|
| Категория уязвимого продукта | Прикладное программное обеспечение |
| Уязвимый продукт | Google Chrome: 90.0.4430.72, 90.0.4430.85, 90.0.4430.93, 90.0.4430.212, 91.0.4472.77, 91.0.4472.101, 91.0.4472.106, 91.0.4472.114, 91.0.4472.124, 91.0.4472.164, 92.0.4515.107, 92.0.4515.131 |
| Дата выявления | 17 августа 2021 г. |
| Дата обновления | 17 августа 2021 г. |

| Идентификатор уязвимости | Описание уязвимости | Базовый уровень CVSS |
|---|---|---|
| MITRE:<br>CVE-2021-30598<br>CVE-2021-30599 | 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:<br>CVE-2021-30600<br>CVE-2021-30601<br>CVE-2021-30602 | 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-2021-30603 | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена состоянием гонки в WebAudio.<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-362: Одновременное использование общих ресурсов при выполнении кода без соответствующей синхронизации (состояние гонки)<br>Рекомендации по устранению: обновить программное обеспечение | 8.8 |
| MITRE:<br>CVE-2021-30604 | 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 |

| | |
|---|---|
| Ссылки на источники | https://bugs.chromium.org/p/chromium/issues/detail?id=1234764<br>https://bugs.chromium.org/p/chromium/issues/detail?id=1234770<br>https://bugs.chromium.org/p/chromium/issues/detail?id=1234009<br>https://bugs.chromium.org/p/chromium/issues/detail?id=1233564<br>https://bugs.chromium.org/p/chromium/issues/detail?id=1230767<br>https://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop.html<br>https://www.cybersecurity-help.cz/vdb/SB2021081702<br>https://bugs.chromium.org/p/chromium/issues/detail?id=1234829<br>https://bugs.chromium.org/p/chromium/issues/detail?id=1231134 |