НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20210716.6 | 16 июля 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в Google Chrome

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Google Chrome: 70.0.3538.67, 70.0.3538.77, 70.0.3538.102, 70.0.3538.110, 71.0.3578.80, 71.0.3578.98, 72.0.3626.81, 72.0.3626.96, 72.0.3626.109, 72.0.3626.119, 72.0.3626.121, 73.0.3683.75, 73.0.3683.86, 73.0.3683.103, 74.0.3729.108, 74.0.3729.131, 74.0.3729.157, 74.0.3729.169, 75.0.3770.80, 75.0.3770.90, 75.0.3770.100, 75.0.3770.142, 76.0.3809.87, 76.0.3809.100, 76.0.3809.132, 77.0.3865.75, 77.0.3865.90, 77.0.3865.120, 78.0.3904.70, 78.0.3904.87, 78.0.3904.97, 78.0.3904.108, 79.0.3945.79, 79.0.3945.88, 79.0.3945.117, 79.0.3945.130, 80.0.3987.87, 80.0.3987.100, 80.0.3987.106, 80.0.3987.116, 80.0.3987.122, 80.0.3987.132, 80.0.3987.149, 80.0.3987.162, 80.0.3987.163, 81.0.4044.92, 81.0.4044.113, 81.0.4044.122, 81.0.4044.129, 81.0.4044.138, 83.0.4103.61, 83.0.4103.97, 83.0.4103.106, 83.0.4103.116, 84.0.4147.89, 84.0.4147.105, 84.0.4147.125, 84.0.4147.135, 85.0.4183.83, 85.0.4183.102, 85.0.4183.121, 86.0.4240.75, 86.0.4240.111, 86.0.4240.183, 86.0.4240.193, 86.0.4240.198, 87.0.4280.66, 87.0.4280.88, 87.0.4280.141, 88.0.4324.96, 88.0.4324.104, 88.0.4324.146, 88.0.4324.150, 88.0.4324.182, 88.0.4324.190, 89.0.4389.72, 89.0.4389.82, 89.0.4389.90, 89.0.4389.114, 89.0.4389.128, 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
Дата выявления	15 июля 2021 г.
Дата обновления	15 июля 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-30559	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти при обработке HTML-данных в ANGLE. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-787: Запись за границами буфера Рекомендации по устранению: обновить программное обеспечение	8.8
MITRE: CVE-2021-30541	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 в компоненте V8. 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: обновить программное обеспечение	8.8
MITRE: CVE-2021-30560	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 в компоненте Blink XSLT. 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: обновить программное обеспечение	8.8

MITRE: CVE-2021-30561	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой смешения типов в компоненте V8. 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: обновить программное обеспечение	8.8
MITRE: CVE-2021-30562	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 в компоненте WebSerial. 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: обновить программное обеспечение	8.8
MITRE: CVE-2021-30563	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой смешения типов в компоненте V8. 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: обновить программное обеспечение	8.8

MITRE: CVE-2021-30564	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти при обработке HTML-данных в WebXR. CVSSv3.0: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H CWE-122: Переполнение буфера в динамической памяти Рекомендации по устранению: обновить программное обеспечение	7.5

Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2021071511 https://crbug.com/1228407 https://crbug.com/1219630 https://crbug.com/1221309 https://crbug.com/1219209 https://crbug.com/1214842 https://crbug.com/1220078 https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop.html https://crbug.com/1219082