НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220305.4 | 5 марта 2022 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Google Chrome

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Google Chrome: 70.0.3538.67 - 98.0.4758.102
Дата выявления	04 марта 2022 г.
Дата обновления	04 марта 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-0800	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольной код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти. CVSSv3.0: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-122: Переполнение буфера в динамической 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.	7.5

MITRE: CVE-2022-0801 CVE-2022-0802 CVE-2022-0803 CVE-2022-0804 CVE-2022-0807	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной реализацией проверок безопасности. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H/E:U/RL:O/RC:C CWE-358: Некорректная реализация стандартизированных проверок безопасности 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.	8.1
MITRE: CVE-2022-0789	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольной 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:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-122: Переполнение буфера в динамической 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.	8.8
MITRE: CVE-2022-0797	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольной 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:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C 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.	8.8

MITRE: CVE-2022-0790 CVE-2022-0791 CVE-2022-0793 CVE-2022-0794 CVE-2022-0796	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольной 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/E:U/RL:O/RC:C 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-2022-0795	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольной код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой смешения типов. 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-843: Доступ к ресурсам с использованием несовместимых типов (смешение типов) 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	https://www.cybersecurity-help.cz/vdb/SB2022030401 http://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html http://crbug.com/1274077 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0790 http://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html http://crbug.com/1278322 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0791 http://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html http://crbug.com/1291728 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0793 http://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html

http://crbug.com/1294097
http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0794
http://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html
http://crbug.com/1282782
http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0795
http://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html
http://crbug.com/1295786
http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0796
http://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html
http://crbug.com/1281908
http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0797
http://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html
http://crbug.com/1289383
http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0789
http://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html
http://crbug.com/1231037
http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0801
http://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html
http://crbug.com/1270052
http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0802
http://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html
http://crbug.com/1280233
http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0803
http://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html
http://crbug.com/1264561
http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0804
http://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html
http://crbug.com/1287364
http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0807
http://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html
http://crbug.com/1242962
http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0800