НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200522.7 | 22 мая 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Google Chrome

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	Google Chrome до v83.0.4103.61
Дата выявления	19 мая 2020 г.
Дата обновления	20 мая 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-6465	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированной вредоносной веб-страницы. Уязвимость обусловлена отсутствием обнуления указателей на освобожденные ячейки буфера памяти в режиме чтения в Google Chrome 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: обновить программное обеспечение.	8.8

MITRE: CVE-2020-6466	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированной вредоносной веб-страницы. Уязвимость обусловлена отсутствием обнуления указателей на освобожденные ячейки буфера памяти в медиа-компоненте Google Chrome 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: обновить программное обеспечение.	8.8
MITRE: CVE-2020-6467	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированной вредоносной веб-страницы. Уязвимость обусловлена отсутствием обнуления указателей на освобожденные ячейки буфера памяти в компоненте WebRTC в Google Chrome 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: обновить программное обеспечение.	8.8
MITRE: CVE-2020-6468	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированной вредоносной веб-страницы. Уязвимость обусловлена ошибкой смешения типов данных в компоненте V8 в Google Chrome 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: обновить программное обеспечение.	8.8

MITRE: CVE-2020-6469	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством открытия пользователем специально сформированной вредоносной веб-страницы. Уязвимость обусловлена некорректной политикой безопасности в инструментах разработчика в Google Chrome. 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-264: Уязвимость в управлении доступом, привилегиями и разрешениями Рекомендации по устранению: обновить программное обеспечение.	8.8

Ссылки на источники	https://chromereleases.googleblog.com/2020/05/stable-channel-update-for-desktop_19.html https://www.cybersecurity-help.cz/vdb/SB2020051918