НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20201112.5 | 12 ноября 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Google Chrome

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Google Chrome до v86.0.4240.198.
Дата выявления	11 ноября 2020 г.
Дата обновления	11 ноября 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-16013	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной обработкой JavaScript в компоненте V8. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C CWE-358: Некорректная реализация стандартизированных проверок безопасности Рекомендации по устранению: обновить программное обеспечение.	8.8

MITRE: CVE-2020-16017	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 при включенной функции «Изоляции сайта» в Google Chrome. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C CWE-416: Использование после освобождения Рекомендации по устранению: обновить программное обеспечение.	8.8

Ссылки на источники	https://chromereleases.googleblog.com/2020/11/stable-channel-update-for-desktop_11.html https://www.zdnet.com/article/google-patches-two-more-chrome-zero-days/