НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200827.2| 27 августа 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости	MITRE: CVE-2020-6492
Идентификатор программной ошибки	CWE-416: Использование после освобождения
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в контексте процесса уязвимого приложения посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной обработкой объектов в памяти компонентом WebGL.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Google Chrome v73 до v84
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	24 августа 2020 г.
Дата обновления	24 августа 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	8.3 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:L
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Требуется (R)
Масштаб последствий эксплуатации уязвимости (S)	Не изменяется (U)
Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Высокое (H)

Влияние на доступность (A)	Низкое (L)
Степень зрелости доступных средств эксплуатации	Концептуальное подтверждение
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://threatpost.com/google-fixes-high-severity-chrome-browser-code-execution-bug/158600/ https://talosintelligence.com/vulnerability_reports/TALOS-2020-1085