

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ
VULN-20191224.3 | 24 декабря 2019 г.
Уровень опасности: **ВЫСОКИЙ**
Наличие обновления: **ЕСТЬ**

Удаленное выполнение кода в web-браузере Google Chrome

Идентификатор уязвимости	MITRE: CVE-2019-13734
Идентификатор программной ошибки	CWE-787: Запись за границами буфера
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному не аутентифицированному злоумышленнику выполнять произвольный код в целевой системе посредством открытия пользователем вредоносной HTML-страницы. Уязвимость обусловлена некорректной работой СУБД SQLite.
Категория уязвимого продукта	Периферийное оборудование
Уязвимое ПО	Google Chrome до v 79.0.3945.79
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	10 декабря 2019 г.
Дата обновления	16 декабря 2019 г.
Оценка критичности уязвимости (CVSSv3)	8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
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)	Высокое (H)
Степень зрелости доступных средств эксплуатации (E)	Наличие не подтверждено (U)
Наличие средств устранения уязвимости (RL)	Официальное решение (O)
Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)
Ссылки на источники	https://nvd.nist.gov/vuln/detail/CVE-2019-13734 https://www.securitylab.ru/news/503683.php https://chromereleases.googleblog.com/2019/12/stable-channel-update-for-desktop.html