

# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200605.1 | 5 июня 2020 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

## Множественные уязвимости в ПО Google Chrome

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	Google Chrome до v83.0.4103.97
Дата выявления	3 июня 2020 г.
Дата обновления	3 июня 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-6493	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой использования памяти после освобождения в компоненте WebAuthentication.</p> <p>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</p> <p>Рекомендации по устранению: обновить программное обеспечение.</p>	8.8

<p>MITRE: CVE-2020-6494</p>	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной проверкой введенных пользователем данных при оплате в Google Chrome.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:U/RL:O/RC:C CWE-451: Некорректное представление важной информации интерфейсом пользователя</p> <p>Рекомендации по устранению: обновить программное обеспечение.</p>	<p>8.1</p>
<p>MITRE: CVE-2020-6495</p>	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику обойти ограничения безопасности в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной политикой безопасности в инструментах разработчика в Google Chrome.</p> <p>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</p> <p>Рекомендации по устранению: обновить программное обеспечение.</p>	<p>8.8</p>
<p>MITRE: CVE-2020-6496</p>	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой использования памяти после освобождения в компоненте платежей в Google Chrome.</p> <p>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</p> <p>Рекомендации по устранению: обновить программное обеспечение.</p>	<p>8.8</p>

Ссылки на  
источники

<https://chromereleases.googleblog.com/2020/06/stable-channel-update-for-desktop.html>  
<https://www.cybersecurity-help.cz/vdb/SB2020060319>