

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20211216.7 | 16 декабря 2021 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Множественные уязвимости в Google Chrome

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Google Chrome: до 96.0.4664.45
Дата выявления	6 декабря 2021 г.
Дата обновления	7 декабря 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-4055 CVE-2021-4058 CVE-2021-4062	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти.</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</p> <p>CWE-122: Переполнение буфера в динамической памяти</p> <p>Рекомендации по устранению: обновить программное обеспечение</p>	8.8

<p>MITRE: CVE-2021-4052 CVE-2021-4053 CVE-2021-4057 CVE-2021-4063 CVE-2021-4064 CVE-2021-4065 CVE-2021-4067</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 после освобождения.</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</p> <p>CWE-416: Использование после освобождения</p> <p>Рекомендации по устранению: обновить программное обеспечение</p>	<p>8.8</p>
<p>MITRE: CVE-2021-4066</p>	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного запроса. Уязвимость обусловлена целочисленным переполнением.</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</p> <p>CWE-191: Потеря значимости целых чисел (простой или циклический возврат)</p> <p>Рекомендации по устранению: обновить программное обеспечение</p>	<p>8.8</p>
<p>MITRE: CVE-2021-4056 CVE-2021-4061</p>	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой смешения типов.</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</p> <p>CWE-843: Доступ к ресурсам с использованием несовместимых типов (смешение типов)</p> <p>Рекомендации по устранению: обновить программное обеспечение</p>	<p>8.8</p>
<p>MITRE: CVE-2021-4059</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 входных данных.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C</p> <p>CWE-20: Некорректная проверка входных данных</p> <p>Рекомендации по устранению: обновить программное обеспечение</p>	<p>7.5</p>

MITRE: CVE-2021-4054	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику подделать содержимое веб-страницы посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной проверкой входных данных при автозаполнении.</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</p> <p>CWE-451: Некорректное представление важной информации интерфейсом пользователя</p> <p>Рекомендации по устранению: обновить программное обеспечение</p>	8.1
-------------------------	--	-----

Ссылки на источники	<p>https://www.cybersecurity-help.cz/vdb/SB2021120701</p> <p>http://chromereleases.googleblog.com/2021/12/stable-channel-update-for-desktop.html</p> <p>http://crbug.com/1272403</p> <p>http://crbug.com/1274641</p> <p>http://crbug.com/1274499</p> <p>http://crbug.com/1273674</p> <p>http://crbug.com/1273197</p> <p>http://crbug.com/1273176</p> <p>http://crbug.com/1271456</p> <p>http://crbug.com/1267661</p> <p>http://crbug.com/1270990</p> <p>http://crbug.com/1267496</p> <p>http://crbug.com/1262183</p> <p>http://crbug.com/1267791</p> <p>http://crbug.com/1239760</p> <p>http://crbug.com/1266510</p> <p>http://crbug.com/1260939</p>	
---------------------	--	--