

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20210112.3 | 12 января 2021 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Множественные уязвимости в Google Chrome

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Google Chrome до v.87.0.4280.141
Дата выявления	7 января 2021 г.
Дата обновления	7 января 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: Не определен	<p>Эксплуатация уязвимости позволяет удалённому злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированной вредоносной веб-страницы. Уязвимость обусловлена некорректным определением границы памяти при обработке входных данных.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C CWE-119: Выполнение операций за пределами буфера памяти</p> <p>Рекомендации по устранению: обновить программное обеспечение.</p>	8.8

<p>MITRE: CVE-2021-21106 CVE-2021-21107 CVE-2021-21108 CVE-2021-21109 CVE-2021-21110 CVE-2021-21112 CVE-2021-21114 CVE-2021-21115</p>	<p>Эксплуатация уязвимости позволяет удалённому злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированной вредоносной веб-страницы. Уязвимость обусловлена некорректным использованием памяти в компонентах уязвимого программного обеспечения.</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>
<p>MITRE: CVE-2021-21113 CVE-2021-21116</p>	<p>Эксплуатация уязвимости позволяет удалённому злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированной вредоносной веб-страницы. Уязвимость обусловлена некорректной обработкой объектов в памяти приложения.</p> <p>CVSSv3.0: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-122: Переполнение буфера в динамической памяти</p> <p>Рекомендации по устранению: обновить программное обеспечение.</p>	<p>7.5</p>
<p>MITRE: CVE-2020-15995</p>	<p>Эксплуатация уязвимости позволяет удалённому злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированной вредоносной веб-страницы. Уязвимость обусловлена некорректной обработкой содержимого HTML-страниц.</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-787: Запись за границами буфера</p> <p>Рекомендации по устранению: обновить программное обеспечение.</p>	<p>8.8</p>

MITRE: CVE-2020-16043	<p>Эксплуатация уязвимости позволяет удалённому злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированной 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 CWE-20: Некорректная проверка входных данных</p> <p>Рекомендации по устранению: обновить программное обеспечение.</p>	8.8
MITRE: CVE-2021-21111	<p>Эксплуатация уязвимости позволяет удалённому злоумышленнику получить НСД к целевой системе посредством открытия пользователем специально сформированной вредоносной веб-страницы. Уязвимость обусловлена некорректной настройкой политик безопасности для веб-интерфейса приложения.</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>	8.8

Ссылки на
источники

<https://www.cybersecurity-help.cz/vdb/SB2021010701>