

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220914.20 | 14 сентября 2022 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Множественные уязвимости в Chrome OS LTS

| | |
|------------------------------|------------------------------------|
| Категория уязвимого продукта | UNIX-подобные операционные системы |
| Уязвимый продукт | Chrome OS: до 102.0.5005.177 |
| Дата выявления | 9 сентября 2022 г. |
| Дата обновления | 9 сентября 2022 г. |

| Идентификатор уязвимости | Описание уязвимости | Базовый уровень CVSS |
|---|--|----------------------|
| MITRE: CVE-2022-2296 CVE-2022-2606 CVE-2022-2607 CVE-2022-2609 CVE-2022-2857 CVE-2022-2998 CVE-2022-3042 CVE-2022-3039 CVE-2022-3046 | <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: данная уязвимость устраняется официальным патчем вендора. в связи со сложившейся обстановкой и введенными санкциями против российской федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p> | 8.8 |

| | | |
|---------------------------------|---|------------|
| <p>MITRE: CVE-2022-2624</p> | <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:H/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: данная уязвимость устраняется официальным патчем вендора. в связи со сложившейся обстановкой и введенными санкциями против российской федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p> | <p>7.5</p> |
| <p>MITRE: CVE-2022-2861</p> | <p>Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной реализацией проверок безопасности.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H/E:U/RL:O/RC:C</p> <p>CWE-358: Некорректная реализация стандартизированных проверок безопасности</p> <p>Рекомендации по устранению: данная уязвимость устраняется официальным патчем вендора. в связи со сложившейся обстановкой и введенными санкциями против российской федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p> | <p>8.1</p> |
| <p>MITRE: CVE-2022-3075</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:R/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C</p> <p>CWE-20: Некорректная проверка входных данных</p> <p>Рекомендации по устранению: данная уязвимость устраняется официальным патчем вендора. в связи со сложившейся обстановкой и введенными санкциями против российской федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p> | <p>8.8</p> |

Ссылки на
источники

<http://chromereleases.googleblog.com/2022/09/long-term-support-candidate-channel-for.html>
