НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20230306.4 | 6 марта 2023 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Chrome OS и Google ChromeOS LTS-102

Категория уязвимого продукта	UNIX-подобные операционные системы
Уязвимый продукт	Chrome OS: до 102.0.5005.197 Chrome OS: до 108.0.5359.221
Дата выявления	5 марта 2023 г.
Дата обновления	5 марта 2023 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2023-0128	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. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H CWE-416: Использование после освобождения 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.	8.8

MITRE: CVE-2022-4139	Эксплуатация уязвимости позволяет аутентифицированному локальному злоумышленнику выполнить произвольный код с повышенными привилегиями в целевой системе. Уязвимость обусловлена ошибкой границ памяти. CVSSv3.0: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H CWE-119: Выполнение операций за пределами буфера памяти 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.	7.8
MITRE: CVE-2022-4378	Эксплуатация уязвимости позволяет аутентифицированному локальному злоумышленнику выполнить произвольный код с повышенными привилегиями в целевой системе. Уязвимость обусловлена ошибкой границ памяти. CVSSv3.0: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H CWE-121: Переполнение буфера в стеке 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.	7.8
MITRE: CVE-2022-45934	Эксплуатация уязвимости позволяет аутентифицированному локальному злоумышленнику выполнить произвольный код с повышенными привилегиями в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена целочисленным переполнением. CVSSv3.0: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H CWE-190: Целочисленное переполнение или циклический возврат 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.	7.8

Ссылки на источники	http://chromereleases.googleblog.com/2023/03/long-term-support-channel-update-for.html