НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20201027.4 | 27 октября 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: НЕТ

Множественные уязвимости в Google Chrome

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Google Chrome: **v**86.0.4240.0 – **v**86.0.4240.110 FreeType: **v**2.0 – **v**2.10.3
Дата выявления	21 октября 2020 г.
Дата обновления	21 октября 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-16000	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством открытия пользователем специально сформированной вредоносной веб-страницы. Уязвимость обусловлена некорректным функционированием компонента Blink в Google Chrome. 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-358: Некорректная реализация стандартизированных проверок безопасности Рекомендации по устранению: обновить программное обеспечение.	7.5

MITRE: CVE-2020-16001 CVE-2020-16002	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством открытия пользователем специально сформированной вредоносной веб-страницы. Уязвимость обусловлена некорректным функционированием медиакомпонента в Google Chrome. 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 Рекомендации по устранению: обновить программное обеспечение.	8.8
MITRE: CVE-2020-15999	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством открытия пользователем специально сформированной вредоносной веб-страницы. Уязвимость обусловлена некорректной обработкой TTF-файлов библиотекой FreeType. 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-122: Переполнение буфера в динамической памяти Рекомендации по устранению: обновить программное обеспечение.	8.8

Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2020102102