НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200923.2 | 23 сентября 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Google Chrome

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Google Chrome: версии с 85.0.4183.0 по 85.0.4183.120
Дата выявления	21 сентября 2020 г.
Дата обновления	22 сентября 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-15960	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной обработкой недоверенного содержимого HTML-страниц компонентом storage. 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

MITRE: CVE-2020-15961 CVE-2020-15962 CVE-2020-15963	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством открытия пользователем специально созданного вредоносного веб-сайта. Уязвимость обусловлена некорректным применением политик безопасности. 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 Рекомендации по устранению: обновить программное обеспечение.	8.8
MITRE: CVE-2020-15965	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена смешением типов компонентом V8. 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-843:Доступ к ресурсам с использованием несовместимых типов (Смешение типов) Рекомендации по устранению: обновить программное обеспечение.	8.8
MITRE: N/A	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректным управлением памятью при обработке HTML-содержимого. 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-119:Выполнение операций за пределами буфера памяти Рекомендации по устранению: обновить программное обеспечение.	8.8

Ссылки на источники	https://chromereleases.googleblog.com/2020/09/stable-channel-update-for-desktop_21.html