НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20210917.2 | 17 сентября 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Microsoft Edge

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Google Chromium: 93.0.4577.0, 93.0.4577.1, 93.0.4577.2, 93.0.4577.3, 93.0.4577.4, 93.0.4577.5, 93.0.4577.6, 93.0.4577.7, 93.0.4577.8, 93.0.4577.9, 93.0.4577.10, 93.0.4577.11, 93.0.4577.12, 93.0.4577.13, 93.0.4577.14, 93.0.4577.15, 93.0.4577.16, 93.0.4577.17, 93.0.4577.18, 93.0.4577.19, 93.0.4577.20, 93.0.4577.21, 93.0.4577.22, 93.0.4577.23, 93.0.4577.24, 93.0.4577.25, 93.0.4577.26, 93.0.4577.27, 93.0.4577.28, 93.0.4577.29, 93.0.4577.30, 93.0.4577.31, 93.0.4577.32, 93.0.4577.33, 93.0.4577.34, 93.0.4577.35, 93.0.4577.36, 93.0.4577.37, 93.0.4577.38, 93.0.4577.39, 93.0.4577.40, 93.0.4577.41, 93.0.4577.42, 93.0.4577.43, 93.0.4577.44, 93.0.4577.45, 93.0.4577.46, 93.0.4577.47, 93.0.4577.48, 93.0.4577.49, 93.0.4577.50, 93.0.4577.51, 93.0.4577.52, 93.0.4577.53, 93.0.4577.54, 93.0.4577.55, 93.0.4577.56, 93.0.4577.57, 93.0.4577.58, 93.0.4577.59, 93.0.4577.60, 93.0.4577.61, 93.0.4577.62, 93.0.4577.63, 93.0.4577.64, 93.0.4577.65, 93.0.4577.66, 93.0.4577.67, 93.0.4577.68, 93.0.4577.69
Дата выявления	13 сентября 2021 г.
Дата обновления	17 сентября 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS

MITRE: CVE-2021-30633 CVE-2021-30625 CVE-2021-30629	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректным освобождением памяти. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C CWE-416: Использование после освобождения Рекомендации по устранению: обновить программное обеспечение	8.8
MITRE: CVE-2021-30626	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти. 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
MITRE: CVE-2021-30627 CVE-2021-30631	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой в работе с типизацией данных. 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: CVE-2021-30628	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти. 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-121: Переполнение буфера в стеке Рекомендации по устранению: обновить программное обеспечение	8.8

MITRE: CVE-2021-30630	Эксплуатация уязвимости позволяет удаленному злоумышленнику посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной обработкой входящих данных. 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

Ссылки на источники	https://crbug.com/1241123 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30633 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30630 https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop.html https://crbug.com/1245786 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30628 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30627 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30631 https://crbug.com/1237533 https://crbug.com/1243646 https://www.cybersecurity-help.cz/vdb/SB2021091704 https://crbug.com/1246932 https://crbug.com/1244568 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30629 https://crbug.com/1241036 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30626 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30625 https://crbug.com/1247766