НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20210906.1 | 6 сентября 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в Microsoft Edge

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Microsoft Edge (Chromium-based): 79.0.309.71, 83.0.478.37, 84.0.522.40, 86.0.622.43, 86.0.622.48, 86.0.622.51, 86.0.622.56, 86.0.622.58, 86.0.622.61, 86.0.622.63, 86.0.622.68, 86.0.622.69, 87.0.664.41, 87.0.664.47, 87.0.664.52, 87.0.664.55, 87.0.664.57, 87.0.664.60, 87.0.664.66, 87.0.664.75, 88.0.705.50, 88.0.705.53, 88.0.705.56, 88.0.705.62, 88.0.705.63, 88.0.705.68, 88.0.705.74, 88.0.705.81, 89.0.774.45, 89.0.774.48, 89.0.774.50, 89.0.774.54, 89.0.774.57, 89.0.774.63, 89.0.774.68, 89.0.774.75, 89.0.774.76, 89.0.774.77, 90.0.818.39, 90.0.818.41, 90.0.818.42, 90.0.818.46, 90.0.818.49, 90.0.818.51, 90.0.818.56, 90.0.818.62, 90.0.818.66, 91.0.864.37, 91.0.864.41, 91.0.864.48, 91.0.864.54, 91.0.864.59, 91.0.864.64, 91.0.864.67, 91.0.864.71, 92.0.902.55, 92.0.902.62, 92.0.902.67, 92.0.902.73, 92.0.902.78, 92.0.902.84
Дата выявления	2 сентября 2021 г.
Дата обновления	2 сентября 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS

MITRE: CVE-2021-30606 CVE-2021-30607 CVE-2021-30608 CVE-2021-30609 CVE-2021-30610	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/E:U/RL:O/RC:C CWE-416: Использование после освобождения Рекомендации по устранению: обновить программное обеспечение	8.8
MITRE: CVE-2021-30614	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:H/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	7.5
MITRE: CVE-2021-30615	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить доступ к конфиденциальной информации на целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной передачей внутренних данных службой Navigation. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C CWE-200: Разглашение важной информации лицам без соответствующих прав Рекомендации по устранению: обновить программное обеспечение	7.5
MITRE: CVE-2021-30618	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить доступ к конфиденциальной информации на целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной реализацией инструментов разработчика. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H/E:U/RL:O/RC:C CWE-358: Некорректная реализация стандартизированных проверок безопасности Рекомендации по устранению: обновить программное обеспечение	8.1

Ссылки на источники	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30624 https://www.cybersecurity-help.cz/vdb/SB2021090211