НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220204.2 | 4 февраля 2022 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости Microsoft Edge (Chromium-based)

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Microsoft Edge (Chromium-based): 79.0.309.71, 79.0.3945.130, 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, 93.0.961.38, 93.0.961.44, 93.0.961.47, 93.0.961.52, 94.0.992.31, 94.0.992.37, 94.0.992.38, 94.0.992.47, 94.0.992.50, 94.0.992.57, 94.0.992.58, 95.0.1020.30, 95.0.1020.38, 95.0.1020.40, 95.0.1020.44, 95.0.1020.53, 96.0.1054.29, 96.0.1054.34, 96.0.1054.41, 96.0.1054.43, 96.0.1054.53, 96.0.1054.57, 96.0.1054.62, 96.0.1054.72, 96.0.1054.75, 97.0.1072.55, 97.0.1072.62, 97.0.1072.69, 97.0.1072.76
Дата выявления	1 февраля 2022 г.
Дата обновления	4 февраля 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-0459 CVE-2022-0452 CVE-2022-0453 CVE-2022-0456 CVE-2022-0458	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-2022-23263	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена некорректной проверкой входных 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-94: Некорректное управление генерированием кода (внедрение кода) Рекомендации по устранению: обновить программное обеспечение	8.8
MITRE: CVE-2022-0454	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-122: Переполнение буфера в динамической памяти Рекомендации по устранению: обновить программное обеспечение	8.8
MITRE: CVE-2022-0455	Эксплуатация уязвимости позволяет удаленному злоумышленнику скомпрометировать целевую систему посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной реализации полноэкранного режима. CVSSv3.0: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	7.5

	CWE-358: Некорректная реализация стандартизированных проверок безопасности Рекомендации по устранению: обновить программное обеспечение	
MITRE: CVE-2022-0457	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой смешения типов. 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-2022-0462 CVE-2022-0466 CVE-2022-0467	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к данным в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной реализацией Scroll. 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://www.cybersecurity-help.cz/vdb/SB2022020404 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0452 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0467 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0462 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0457 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0459 http://crbug.com/1287962 http://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop.html http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0453 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0454 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0456

http://crbug.com/1267060
http://crbug.com/1270470
http://crbug.com/1115460
http://crbug.com/1270593
http://crbug.com/1239496
http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0455
http://crbug.com/1244205
http://crbug.com/1289523
http://crbug.com/1284916
http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0458
http://crbug.com/1284584
http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0466
http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23263
http://crbug.com/1274445