Махонина Е. А., Верас Н. А., Коньков В. В. Исследование уязвимости браузера Microsoft Edge операционных систем Windows BDU:2022-06064 // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 4(26) часть 1 с. 27–30

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.7

ИССЛЕДОВАНИЕ УЯЗВИМОСТИ БРАУЗЕРА MICROSOFT EDGE ОПЕРАЦИОННЫХ СИСТЕМ WINDOWS BDU:2022-06064

[1]Махонина Е. А., [2]Верас Н. А., [3]Коньков В. В.
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, г.Санкт-Петербург, Российская Федерация (193232, г. Санкт-Петербург, пр. Большевиков, 22, к. 1), e-mail: [1]Makhonina800@mail.ru, [2]Veras.good@bk.ru, [3]1568487@yandex.ru

В статье рассмотрена уязвимость браузера Microsoft Edge операционных систем Windows BDU:2022-06064, приведено описание актуальных угроз, основанных на использовании уязвимости. Приводятся описания способов предотвращения нарушений информационной безопасности, а также зафиксированных случаев сетевых атак, проведенных при эксплуатации злоумышленником уязвимости.

Ключевые слова: информационная безопасность, веб-браузер, Windows, утечки информации.

VULNERABILITY STUDY OF THE MICROSOFT EDGE BROWSER FOR WINDOWS OPERATING SYSTEMS BDU:2022-06064

[1]Makhonina E.A., [2]Veras N.A., [3]Konkov V.V.
St. Petersburg State University of Telecommunications named after M.V. prof. M.A. Bonch-Bruevich, St. Petersburg, Russia (193232, St. Petersburg, pr. Bolsheviks, 22, building 1), e-mail: [1]Makhonina800@mail.ru, [2]Veras.good@bk.ru, [3]1568487@yandex.ru

The article discusses the vulnerability of the Microsoft Edge browser of Windows operating systems BDU:2022-06064, provides a description of current threats based on the exploitation of the vulnerability. Descriptions are given of ways to prevent information security violations, as well as recorded cases of network attacks carried out when an attacker exploited a vulnerability.

Keywords: information security, web browser, Windows, information loss.

Введение

В настоящее время существует всеобъемлющая потребность пользователей в безопасном использовании веб-ресурсов, а поиск и устранение уязвимостей веб-браузеров являются важными задачами в сфере информационной безопасности. Поэтому исследование уязвимости BDU:2022-06064 является актуальным.

Целью исследования является изучение и описание уязвимости, выявление эффективных решений для борьбы с атаками и утечкой защищаемой информации, возникающими при эксплуатации уязвимости, а также исследование зафиксированных случаев нарушения информационной безопасности с использованием таких атак.

Объектом исследования является уязвимость браузера Microsoft Edge с точки зрения возможности проведения спуфинг-атак, при ее выявлении.

Статья нацелена на студентов технических учебных заведений, специалистов, работающих с сетевыми технологиями, а также читателей, которым интересна данная тематика.

Новизна исследования состоит в обобщении изученной литературы, а также данных, публикуемых компаниями по разработке веб-браузеров на тему уязвимостей в сети Интернет, а также изучение отечественных решений по борьбе со спуфинг-атаками.

Описание уязвимости

Уязвимость браузера Microsoft Edge операционных систем Windows Уязвимость браузера Microsoft Edge возникает из-за ошибок синхронизации при использовании общего ресурса («ситуация гонки»). Использование данной уязвимости позволяет нарушителям проводить спуфинг-атаки. Уязвимость имеет высокий уровень опасности (базовая оценка CVSS 3.0 составляет 8,1). Уязвимость подтверждена производителем и описывается как, переполнение буфера кучи в графическом процессоре в Google Chrome до 107.0.5304.121, что позволяет удаленному злоумышленнику, скомпрометировавшему процесс рендеринга, потенциально выполнить выход из песочницы через созданную HTML-страницу и имеет идентификатор CVE-2022-4135. По шкале серьезности опасности Chromium уязвимость также оценивается как высокая.

Меры защиты

1. *Установка обновлений из доверенных источников.*

3 октября 2022 г. компания Microsoft выпустила последнюю версию Microsoft Edge Stable Channel (version 106.0.1370.34), которая включает в себя обновление безопасности проекта Chromium. В Руководстве по обновлению безопасности задокументировано объявление о том, что последняя версия Microsoft Edge (на основе Chromium) не является уязвимой при одновременном выполнении с использованием общего ресурса. Однако, компания Google в своих источниках сообщает, что эксплойт для CVE-2022-4135 уже существует. Стоит заметить, что установление любых обновлений программного обеспечения возможно только после оценки всех сопутствующих рисков.

2. *Использование средств антивирусной защиты с функцией контроля доступа к веб-ресурсам.*

Антивирусы с функциями контроля использования программ, устройств и веб-ресурсов являются эффективным средством защиты от спуфинг-атак, поэтому целесообразно использование программного обеспечения такого типа для борьбы с угрозами, возникающими на базе уязвимости BDU:2022-06064. В настоящий момент существуют решения отечественных производителей, позволяющие устанавливать Веб-контроль.

3. *Применение систем обнаружения и предотвращения вторжений.*

Такие средства защиты используют метод отслеживания несанкционированных попыток получения доступа к защищаемым ресурсам, называемый мониторингом управления доступом. Задача решений систем обнаружения и предотвращения вторжений состоит в выявлении, а также регистрации уязвимостей в безопасности внутренней инфраструктуры.

Можем выделить и другие эффективные меры защиты, такие как введение регламента по использованию ресурсов сети «Интернет»; отказ от использования запуска браузеров от имени администратора в пользу запуска от имени пользователя минимальными возможными

привилегиями в операционной системе и использование альтернативных веб-браузеров, в которых отсутствует рассматриваемая уязвимость.

Далее будет представлена информация об атаках, которая получена с помощью мониторинга открытых источников в сети Интернет и может не соответствовать действительности [1-3].

Атаки

1. В Telegram-канале (https://t.me/itarmyofukraine2022) с 5 октября 2022 года осуществляется координация DDoS-атаки на сайты российских магазинов торгово-бытового обеспечения военнослужащих «Военторг». Сообщается, что список атакуемых сайтов включает 72 адреса.

2. В Telegram-канале (https://t.me/CyberSquattingChannel) опубликованы

URL-адреса, используемые в атаках с применением социальной инженерии, схожие с адресами интернет-ресурсов крупных российских компаний (такие, как: new-sber.run.app; sberbank.com.cn; sberget.com; sbertibud.cf; sberukmud.ga; investments-gazprom.online; bonus-vtb24-pozdravlenie.site; sushi-for-you-vtb.ru; sushi-tebe-vtb.ru; sushi-vam-vtb.ru; sushi-vsem-vtb.ru; vtb-bonus.site; gosuslugi-r.ru; gosuslugi.vercel.app; gosuslugl.vercel.app; ozon-hd.hu; wb-ozon-obuchenie.ru; yandex-dellivery.net.ru; yandex-leonteva.ru; yandex-oplata37124.online; yandex-oplata37317.online; yandex-yana.ru; cdek-oplata24127.online; cdek-oplatazakaza.online avito.id13860.ru; avito.id7355.ru; avito.id9217.ru; booking.id1704.ru; cdek.id1789523.ru; cdek.id7355.ru; cdek.id7360.ru; cdek.ord-0125.ru; mvd-oplata.top; mvideo.id1704.ru; ozon.id7354.ru; ozon.id7358.ru; wildberries.id47218.ru; wildberries.ord1838.ru; yandex-id8512.ru; youla-paymo.ru; youla.id11327.ru; youla.id13860.ru; youla.id13875.ru; youla.id5755.ru; youla.id7355.ru; youla.id7358.ru; youla.id9215.ru; youla.id9217.ru; youla.id9218.ru) [4].

Заключение

В ходе исследования была изучена научная литература, посвященная уязвимостям в веб-браузерах, а также возможным решениям для предотвращения сетевых атак. Полученные результаты были обобщены, а также была выделена уязвимость BDU:2022-06064, приведены ее основные характеристики. Поставленные цели и задачи были достигнуты в полном объеме. Можно сделать вывод о том, что исследование угроз в сети интернет, в том числе атак, проводимых при использовании веб-браузеров остается важной задачей, стоящей перед специалистами информационной безопасности [5].

Список литературы

1. Волкогонов В. Н., Гельфанд А. М., Деревянко В. С. Актуальность автоматизированных систем управления // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 262-266.
2. Казанцев А. А. и др. Создание и управление Security Operations Center для эффективного применения в реальных условиях //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 590-595.
3. Пестов И. Е. и др. Программа обеспечения системы компьютерного зрения на основе библиотеки OpenCV // Свидетельство о регистрации программы для ЭВМ. – 2020. – № 2020664289

4. Красов А. В. и др. Программная реализация средств предотвращений вторжений и аномалий сетевой инфраструктуры // Свидетельство о регистрации программы для ЭВМ. – 2020. – № 2020617705
5. Методический документ ФСТЭК России Профиль защиты систем обнаружения вторжений уровня узла пятого класса защиты ИТ.СОВ.У5.ПЗ

References

1. Volkogonov V. N., Gelfand A. M., Derevyanko V. S. Relevance of automated control systems // Actual problems of infotelecommunications in science and education (APINO 2019). - 2019. - S. 262-266.
2. Kazantsev A. A. et al. Creation and management of the Security Operations Center for effective use in real conditions // Actual problems of infotelecommunications in science and education (APINO 2019). - 2019. - S. 590-595.
3. Pestov I. E. et al. Program for providing a computer vision system based on the OpenCV library // Certificate of registration of a computer program. - 2020. - № 2020664289
4. Krasov A. V. et al. Software implementation of intrusion and anomality prevention in the network infrastructure // Certificate of registration of a computer program. - 2020. - № 2020617705.
5. Methodological document of the FSTEC of Russia profile of protection of intrusion detection systems of the node level of the fifth protection class IT.SOV.U5.PZ