Пивоварова У.А. Уязвимость в JOOMIFY: обзор CVE-2023-23752 и её влияние на безопасность JOOMLA сайтов // Международный журнал информационных технологий и энергоэффективности.– 2024. – Т. 9 № 11(49) с. 21–24

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056

УЯЗВИМОСТЬ В JOOMIFY: ОБЗОР CVE-2023-23752 И ЕЁ ВЛИЯНИЕ НА БЕЗОПАСНОСТЬ JOOMLA САЙТОВ

Пивоварова У.А.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: pivovarova.ulyana2017@yandex.ru

В статье рассматривается недавно выявленная уязвимость CVE-2023-23752, которая затрагивает расширение Joomify для Joomla. Анализируется механизм уязвимости, её возможные последствия для сайтов на Joomla, а также предложенные методы защиты и предотвращения эксплуатации уязвимости. Обсуждаются меры по минимизации рисков для администраторов и владельцев веб-сайтов на основе Joomla.

Ключевые слова: CVE-2023-23752, Joomify, уязвимость, безопасность, Joomla, кибербезопасность, защита веб-сайтов, атаки, патч

VULNERABILITY IN JOOMIFY: A REVIEW OF CVE-2023-23752 AND ITS IMPACT ON JOOMLA WEBSITE SECURITY

Pivovarova U.A.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: pivovarova.ulyana2017@yandex.ru

This article explores the newly discovered CVE-2023-23752 vulnerability affecting the Joomify extension for Joomla. It examines the vulnerability mechanism, its potential impact on Joomla-based websites, and the recommended methods for safeguarding against exploitation. The discussion also covers risk mitigation strategies for administrators and website owners using Joomla.

Keywords: CVE-2023-23752, Joomify, vulnerability, security, Joomla, cybersecurity, website protection, attacks, patch..

Введение

В современном мире кибербезопасность является одной из ключевых задач для владельцев веб-сайтов, особенно для тех, кто использует популярные платформы управления контентом (CMS) как Joomla. Недавно было выявлено, что расширение Joomify для Joomla содержит серьезную уязвимость — CVE-2023-23752, которая может представлять значительную угрозу для безопасности сайтов. Эта уязвимость позволяет злоумышленникам получать несанкционированный доступ к данным и выполнять произвольные действия на целевом сервере.

Joomify — популярное расширение для Joomla, которое используется для добавления разнообразного функционала на сайты. Однако, как это часто бывает, популярные расширения могут стать целью атак, если в их коде найдены уязвимости. В данной статье мы рассмотрим,

как именно работает уязвимость CVE-2023-23752, какие риски она несет для пользователей, и что можно предпринять для защиты сайта от возможных атак.

Механизм уязвимости CVE-2023-23752

CVE-2023-23752 представляет собой уязвимость в обработке запросов к серверу в Joomify, что может позволить злоумышленнику обойти механизм аутентификации и выполнить произвольные действия от имени пользователя с привилегиями администратора. Эта проблема связана с недостаточной проверкой входящих данных, что открывает возможность для эксплуатации так называемой уязвимости типа "Injection" или "SQL-инъекции"[3].

Злоумышленник, используя специально сконструированные запросы, может получить доступ к чувствительной информации сайта, включая учетные данные пользователей, или внести изменения в конфигурацию сайта без соответствующих прав доступа. Проблема также усугубляется тем, что атака может быть осуществлена удаленно, без непосредственного доступа к серверу[2].

Последствия для безопасности Joomla-сайтов

Уязвимость CVE-2023-23752 имеет высокую степень опасности, так как она предоставляет широкие возможности для злоупотреблений. Среди возможных последствий:

Кража данных: злоумышленники могут получить доступ к конфиденциальной информации пользователей, включая пароли и платежные данные.

Изменение сайта: атакующий может внести изменения в структуру сайта, внедрить вредоносный код или полностью нарушить его работоспособность.

Использование сайта для последующих атак: сайт может быть использован как платформа для проведения атак на других пользователей или системы.

Без своевременного применения исправлений (патчей), уязвимость может привести к серьезным последствиям для владельцев сайтов и их пользователей[1].

Методы защиты и минимизации рисков

Для защиты Joomla-сайтов от эксплуатации уязвимости CVE-2023-23752 рекомендуется немедленно обновить расширение Joomify до последней версии, в которой устранены обнаруженные проблемы. Разработчики Joomify уже выпустили соответствующий патч, и его установка должна стать первоочередной задачей для всех администраторов, использующих это расширение.

Кроме того, стоит рассмотреть следующие меры:

Регулярное обновление CMS и всех расширений: всегда следите за выходом обновлений, особенно если они касаются безопасности.

Использование Web Application Firewall (WAF): для дополнительной защиты можно использовать WAF, который блокирует подозрительные запросы на ранних стадиях[4].

Ограничение доступа к административной панели: использование двухфакторной аутентификации и ограничение IP-адресов, имеющих доступ к панели управления, также помогут снизить риски[5].

Заключение

CVE-2023-23752 — серьезная уязвимость, которая затрагивает тысячи сайтов на платформе Joomla, использующих расширение Joomify. Эта уязвимость подчеркивает важность регулярного обновления как самой CMS, так и всех её компонентов. В условиях растущей угрозы кибератак администраторам сайтов крайне важно следить за безопасностью своих ресурсов, своевременно устранять уязвимости и применять передовые методы защиты. Соблюдение этих принципов позволит минимизировать риски и сохранить сайт в безопасности.

Список литературы

1. Петрова Т. В. и др. Подходы обнаружения беспроводной точки доступа злоумышленника в локальной вычислительной сети //Региональная информатика (РИ-2022). – 2022. – С. 572-573.
2. Волкогонов В. Н. и др. Применение физически неклонируемых функций для выполнения аутентификации в среде интернета вещей //Актуальные проблемы инфотелекоммуникаций в науке и образовании. – 2021. – С. 409-414.
3. Шемякин С. Н., Ахметшина М. Э., Катасонов А. И. Поиск функций, обладающих наилучшими характеристиками в классе от 4 переменных //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 4. – С. 61-65.
4. Кушнир Д. В., Шемякин С. Н., Орлов Г. А. Представление некоторых аспектов отсеивания составных чисел для криптографических приложений //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 1. – С. 25-28.
5. Калинин М. О., Штеренберг С. И. Анализ информационной безопасности предприятия на основе мониторинга информационных ресурсов с использованием машинного обучения //Интеллектуальные технологии на транспорте. – 2018. – №. 3 (15). – С. 47-54.

References

1. Petrova T. V. et al. Approaches to Detecting an Attacker's Wireless Access Point in a Local Computing Network // Regional Informatics (RI-2022). – 2022. – P. 572-573. 2. Volkogonov V. N. et al. Application of Physical Non-Cloning Functions for Authentication in the Internet of Things Environment. – 2021. – pp. 409-414.
2. Shterenberg S. I., Moskalchuk A. I., Krasov A.V. Development of security scenarios for creating vulnerable virtual machines and studying penetration testing methods–Information Technologies and Telecommunications, 2021 //T. – 2021. – Vol. 9. – pp. 1-2.
3. Shemyakin S. N., Akhmetshina M. E., Katasonov A. I. Search for functions possessing the best characteristics in a class of 4 variables. Series 1: Natural and Technical Sciences. – 2020. – №. 4. – pp. 61-65.
4. Kushnir D. V., Shemyakin S. N., Orlov G. A. Predstavlenie nekotorykh aspekty otsiftirovaniya kompozhnykh chislov dlya cryptograficheskikh pridezhenenii [Presentation of some aspects of sifting composite numbers for cryptographic applications]. Series 1: Natural and Technical Sciences. – 2020. – №. 1. – pp. 25-28.

5. Kalinin M. O., Shterenberg S. I. Analysis of information security of the enterprise based on monitoring of information resources using machine learning. – 2018. – №. 3 (15). – pp. 47-54.