Кибербандиты массово внедряют бэкдоры в файлы плагинов и тем оформления.

Исследователи в области кибербезопасности предупредили о том, что несколько серьёзных уязвимостей в плагинах WordPress — это бесплатная платформа для управления контентом веб-сайтов (CMS), которая позволяет пользователям создавать и управлять своими собственными веб-сайтами без необходимости обладать специальными знаниями в области программирования. С помощью WordPress можно создавать различные типы сайтов, включая блоги, интернет-магазины, корпоративные сайты и другие типы веб-ресурсов. Платформа имеет открытый исходный код, что позволяет разработчикам создавать расширения и темы для WordPress, чтобы расширять его функциональность и адаптировать внешний вид сайта под свои нужды." data-html="true" data-original-title="WordPress" >WordPress активно используются злоумышленниками для создания поддельных учётных записей администраторов.

«Эти уязвимости обнаружены в различных плагинах WordPress и подвержены атакам с использованием неаутентифицированных хранимых межсайтовых скриптов (XSS (Cross Site Scripting, межсайтовый скриптинг) – один из типов уязвимостей компьютерной системы, используя которую хакер может внедрить в генерируемую скриптами на сервере HTML-страницу произвольный код. Специфика хакерских атак, с использованием XSS, заключается в том, что вместо атаки, нацеленной на сервер, мошенники используют сервер в качестве средства атаки на клиента.

 Обычно XSS-атаки направлены на хищение личных данных, таких как cookies, паролей и пр. Такая атака также может внедрять код скриптов и ссылок на web-страницы.

 Ранее программисты не уделяли должного внимания XSS-атакам, так они считались неопасными. Однако на web-странице или в HTTP-Cookie могут содержаться потенциально важные данные (к примеру, идентификатор сессии администратора). На популярный сайт при помощи XSS уязвимости можно осуществить DDoS-атаку." data-html="true" data-original-title="XSS" >XSS) из-за недостаточной очистки входных данных и экранирования выходных данных, что позволяет злоумышленникам внедрять вредоносные скрипты», — сообщили исследователи компании Fastly.

Ниже приведены уязвимости, подверженные атакам:

Цепочки атак, использующие эти уязвимости, включают внедрение полезной нагрузки, указывающей на зашифрованный JavaScript-файл, размещённый на внешнем домене. Этот файл создаёт новую учётную запись администратора, вставляет бэкдор и устанавливает скрипты для отслеживания.

Бэкдоры на языке PHP внедряются как в файлы плагинов, так и в файлы тем

оформления, в то время как скрипт отслеживания отправляет HTTP GET запрос с информацией о хосте на удалённый сервер.

WPScan — это подразделение компании Automattic, которая занимается исследованием и обнаружением уязвимостей в плагинах и темах для платформы управления контентом WordPress. Специалисты WPScan работают над поиском и анализом потенциальных угроз безопасности, связанных с WordPress, и разрабатывают инструменты для обнаружения и устранения этих уязвимостей.

 WPscan также представляет из себя одноимённый инструмент для самостоятельного поиска уязвимостей в веб-сайтах, работающих на WordPress. Этот инструмент предоставляет администраторам возможность сканировать собственные сайты на предмет наличия уязвимостей в плагинах, темах и ядре системы." data-html="true" data-original-title="WPscan" >WPScan, компания по безопасности WordPress, ранее раскрывала аналогичные атаки, направленные на CVE-2023-40000, для создания поддельных учётных записей администраторов на уязвимых сайтах.

Для снижения рисков таких атак владельцам сайтов на WordPress рекомендуется проверить установленные плагины, обновить их до последних версий и провести аудит сайтов на наличие вредоносного ПО или подозрительных учётных записей администраторов.