Хакеры стали атаковать сайты, созданные с помощью системы WordPress

С февраля 2025 года специалисты BI. ZONE WAF заметили рост атак на сайты, использующие платформу WordPress. После выхода исследования компании Sucuri, в котором подробно описана уязвимость, количество атак резко увеличилось — за несколько дней было зафиксировано 250 попыток атак на 13 организаций. Причиной таких атак стали проблемы с определённым типом плагинов, которые запускаются на сайте автоматически.

Злоумышленники используют так называемые must-use plugins — плагины, которые не требуют активации и начинают работать сразу при загрузке страницы. Эти плагины хранятся в специальной папке сайта и могут выполнять разные вредоносные действия, такие как перенаправление пользователей на опасные сайты, загрузка вирусов и установка скрытых программ для удалённого контроля над сайтом. По словам специалистов, эта уязвимость представляет собой серьёзную угрозу, поскольку злоумышленники могут получить доступ к сайту и использовать его как «заднюю дверь» для дальнейших атак.

Хотя уязвимость не получила официальной оценки по шкале CVSS, эксперты BI. ZONE считают её критической из-за того, что она позволяет запустить вредоносные программы без активации плагина в панели управления. Кроме того, эта угроза не входит в базу известных уязвимостей CVE, что затрудняет её блокировку с помощью стандартных методов защиты. Чтобы избежать подобных атак, специалисты рекомендуют следить за изменениями в работе сайта и проверять содержимое папки, где хранятся эти плагины. В ответ на угрозу BI. ZONE уже разработали специальные правила для обнаружения и блокировки таких атак.