Советы

Ваш Moodle под угрозой: почему «работает — не трогай» не работает

Уязвимости удаленного выполнения кода или RCE остаются главной угрозой для устаревших версий Moodle, открывая злоумышленникам прямой путь к загрузке веб-шелл, то есть программ или скриптов для удаленного управления, и полному захвату сервера.

Многие администраторы годами не обновляют систему, руководствуясь принципом «студенты учатся, тесты сдаются, зачем что-то менять?». Однако для информационной безопасности такая стабильность — это бомба замедленного действия.

Большинство критических инцидентов, связанных со взломом, развиваются по классическому сценарию:

1. Поиск RCE.
   Преступники используют уязвимости в плохо валидируемых компонентах: через логику восстановления бэкапов, плагины репозиториев или вычисляемые вопросы в тестах атакующий находит способ заставить сервер исполнить его код.
2. Загрузка веб-шелла.
   С помощью RCE-уязвимости в веб-директорию
   СДО загружается вредоносный PHP-скрипт (веб-шелл).
3. Закрепление в системе.
   Через веб-шелл хакеры получают постоянный доступ к серверу. Это позволяет им читать базы данных, красть персональные данные пользователей, шифровать файлы ради выкупа или превращать сервер в базу для атак на внутреннюю сеть организации.

Чтобы предотвратить атаки, защитить учебный процесс и данные, внедрите обязательные правила:

- Регулярные обновления.
  Обновляйте ваш Moodle после выхода стабильной версии, не торопясь переходить на свежие короткоживущие релизы. Каждый стабильный релиз содержит не только новые функции и исправления ошибок, но и обновления безопасности.
- Принцип минимальных привилегий.
  Ограничьте права на создание курсов, загрузку файлов и восстановление бэкапов. Не давайте права администраторов сторонним пользователям.
- Настройка параметров безопасности сайта.
  На странице Администрирование → Безопасность → Параметры безопасности сайта настройте параметры для защиты системы и

пользователей, например, включите и настройте политику паролей и ограничьте квоту пользователя. Это усложнит подбор паролей методом перебора и не позволит перегрузить дисковое пространство на сервере.

- Внимательнее подходите к необходимости установки сторонних плагинов.
  Практически любой сценарий можно реализовать с помощью инструментов, входящих в состав Moodle, а сторонние плагины могут содержать уязвимости и вызывать внутренние ошибки.

Защищайте данные от преступников: обновляйте Moodle вовремя и соблюдайте меры предосторожности.

Либо переходите на СЭО 3KL: мы сами будем заботиться о вашей безопасности и обновлять систему по вашим запросам!

Уникальный ID ответа: #1964
Опубликовал: : Наталья Олейникова
Последние обновление: 2026-08-13 15:42