Автор:
30.10.14 03:59 -

История с выявлением критической уязвимости (CVE-2014-3704) в системе управления web-контентом Drupal получила неожиданное продолжение. Разработчики Drupal опубликовали
экстренное заявление, в котором объявили, что все системы на основе Drupal 7, которые в течение семи часов не успели обновить до версии 7.32, следует считать скомпрометированными. 15 октября в 11 часов (GMT) зафиксировано начало автоматизированной массовой атаки на сайты, в результате которой была развёрнута кампания по скрытой установке бэкдоров.

Обновление уже атакованных систем до версии 7.32 не решает проблемы, бэкдор останется активен. Более того, после внедрения бэкдора в некоторых случаях атакующими производилось применение патча, закрывающего уязвимость для блокирования повторных атак на систему. Иными словами, если на сайте уже закрыта уязвимость, но администратор не применял патчи, то это является одним из индикаторов компрометации. Более того, некоторые виды атак невозможно отследить, так как они не были связаны с изменением кода, а лишь привели к выгрузке содержимого БД, включая базу пользователей. Кроме того, зафиксировано применение различных способов внедрения бэкдора - от изменения содержимого БД до правки PHP-кода, размещения новых PHP-файлов и проведения атак на смежные web-сервисы.

Так как нельзя полностью быть уверенным в отсутствии атаки, пользователям Drupal, которые сразу не установили обновление, рекомендуется изменить пароли и восстановить содержимое своих сайтов из резервной копии, созданной до 15 октября, или провести детальный аудит всех изменений. При этом нельзя исключить, что атакующие могли воспользоваться другими уязвимостями для повышения своих привилегий в системе и их деятельность может не ограничиться атакой на Drupal.

Read more http://www.opennet.ru/opennews/art.shtml?num=40965