



Аудит безопасности сервера для Клиента (ознакомительная версия)

Нашими специалистами был проведен аудит безопасности сервера. По результатам аудита были найдены следы взлома, локализована уязвимость, через которую проник злоумышленник и даны рекомендации по улучшению безопасности сервера.

По логам **/var/log/httpd-access.log** , найдены IP адреса взломщиков: см. файлы «use_shell.txt» и «hack_ip.txt» в архиве.

Результаты аудита сервера

Шелл на сервере
<p>Описание проблемы Найден шелл: /usr/home/www/phpMyAdmin/config/5bn3c.php А также файл: /usr/home/www/phpMyAdmin/config/368r4.php, который, предположительно, использовался для рассылки писем.</p> <p>Решение Права на чтение этих файлов убраны, также в директорию добавлен .htaccess , блокирующий вызов php-файлов. Содержимое .htaccess: <i><убрано в ознакомительной версии отчета></i></p> <p>Рекомендации <i><убрано в ознакомительной версии отчета></i></p>

Уязвимость, через которую был залит шелл
<p>Описание проблемы По логам видно, что злоумышленник использовал файл scripts/setup.php в phpMyAdmin. Файл уязвим: через него можно выполнять произвольные команды php, что и привело к заливке шелла.</p> <p>Решение Права на чтение этих файлов в директории phpMyAdmin/scripts/ убраны, также в директорию добавлен .htaccess , блокирующий вызов php-файлов. Это не нарушает работу phpMyAdmin, но при этом не дает возможности залить шелл. Содержимое .htaccess: <i><убрано в ознакомительной версии отчета></i></p> <p>Рекомендации 1. Обновить phpMyAdmin до новой версии.</p>

2. Использовать нестандартное и сложное имя директории phpMyAdmin, которое будет невозможно подобрать.

Описание проблемы

Из выборки логов по регулярным выражениям видны попытки атак типа LFI и SQL-injection: см. файлы «SQLInj.txt» и» LFI.txt» в архиве.

Рекомендации

<убрано в ознакомительной версии отчета>

Следы злоумышленника

Описание проблемы

В директории /tmp/ присутствуют файлы: a.x , a.x.1 , c , c.1 , c.2 , c.3 , env , env.c , program.c , program.o , udp.pl , w00t.so.1.0. Это эксплойты и скрипт бек-коннекта, для получения доступа к управлению оболочкой типа bash, что говорит о попытке повышения привилегий (т.е. получения root). Скорее всего, попытка неудачная.

Рекомендации

Удалить эти файлы.

Настройка прав сервера

Описание проблемы

Некорректная настройка прав сервера позволяет злоумышленнику получить доступ ко всем сайтам на сервере, имея шелл на любом из них. Это достаточно большой пробел в безопасности.

Рекомендации

<убрано в ознакомительной версии отчета>

Настройка прав php

Рекомендации

Рекомендуемые значения настроек конфигурации php (php.ini):

allow_url_include = Off

disable_functions = phpinfo, system, exec, shell_exec, passthru, popen, proc_open,

pcntl_exec, putenv

open_basedir = /usr/home/www/:/tmp/:/var/tmp/

display_errors = Off

Наши контакты:

Web-site: <http://rebz.net>

E-Mail: support@rebz.net