**Playbook по устранению уязвимости CVE-2021-41773**

**Цель**

Устранение уязвимости CVE-2021-41773 в веб-сервере Apache, которая позволяет злоумышленникам осуществлять атаки обхода каталога и потенциально выполнять произвольный код.

**Шаги по устранению**

1. **Идентификация уязвимых систем**

Проведите инвентаризацию всех серверов, на которых установлен Apache версии 2.4.49 или 2.4.50.

Используйте команду для проверки версии Apache:

apachectl -v

1. **Обновление Apache**

* Обновите Apache до последней стабильной версии (рекомендуется 2.4.51 или выше). Используйте следующие команды в зависимости от вашей операционной системы:

Для Debian/Ubuntu:

sudo apt update

sudo apt install apache2

Для CentOS/RHEL:

* + sudo yum update httpd

1. **Проверка конфигурации**

* Проверьте конфигурацию Apache на наличие директивы Require all denied для защиты файлов за пределами корня документа.
* Убедитесь, что директивы, позволяющие доступ к файловой системе, настроены правильно:

<Directory />

Require all denied

</Directory>

1. **Тестирование уязвимости**

* После обновления проверьте, устранена ли уязвимость, используя тестовую команду:
  + curl --silent --path-as-is --insecure "http://<host>/cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd" | grep -q "root.\*" && echo "Host is vulnerable" || echo "Host is Not vulnerable"

1. **Мониторинг и реагирование**
   * Настройте систему обнаружения вторжений (IDS) для мониторинга попыток эксплуатации данной уязвимости.
   * Обновите сигнатуры IDS для обнаружения атак, связанных с CVE-2021-41773.
2. **Обучение персонала**
   * Проведите обучение для администраторов и сотрудников IT о важности обновления программного обеспечения и соблюдения лучших практик безопасности.
3. **Документация и отчетность**
   * Зафиксируйте все действия по устранению уязвимости в отчетах безопасности.
   * Подготовьте отчет о состоянии безопасности системы после выполнения всех шагов.

**Заключение**

Регулярные обновления программного обеспечения и правильная конфигурация серверов являются ключевыми мерами для защиты от уязвимостей, таких как CVE-2021-41773. Следуя этому playbook, вы сможете эффективно устранить данную уязвимость и минимизировать риски для вашей организации.