Playbook для устранения уязвимости CVE-2021-41773

Исполнитель: Олег Тихоненко **Дата:** 18 января 2025 года

Информация:

- Уязвимость CVE-2021-41773 затрагивает веб-сервер Apache версии 2.4.49 и связана с ошибками в процессе нормализации URL, что позволяет злоумышленникам осуществлять path traversal атаки. Это означает, что злоумышленник может манипулировать URL, чтобы получить доступ к файлам за пределами ожидаемого корня документа (document root) сервера.

Основные характеристики уязвимости:

- Тип атаки: Path Traversal
- Версия Apache: Уязвима только версия 2.4.49.
- Рейтинг CVSS: 7.5 (высокий уровень риска).

Эксплуатация:

- Если сервер неправильно настроен (например, параметр Require all denied отключен), злоумышленник может получить доступ к защищённым файлам и даже выполнять произвольный код, если поддерживается модуль CGI (mod_cgi)

Потенциальные последствия:

- Утечка конфиденциальных данных: Злоумышленники могут получить доступ к критически важным файлам, таким как скрипты CGI.
  Удаленное выполнение кода (RCE): При определенных условиях возможно выполнение произвольного кода на сервере, что может привести к полной компрометации системы.

Рекомендации по устранению:

- Обновить Apache до версии 2.4.50 или выше, где данная уязвимость была исправлена.
- Проверить конфигурацию сервера для обеспечения правильной защиты файлов за пределами document root.

Шаги по устранению уязвимости:

- **Идентификация версии Apache**

  1 Проверьте текущую версию установленного веб-сервера Apache.

  Для этого выполните команду:

  bash
  apache2 -v

  2 Убедитесь, что версия не ниже 2.4.50. Если версия 2.4.49, переходите к следующему шагу.

- **Резервное копирование конфигурации**

  3 Создайте резервную копию текущих конфигурационных файлов Apache:

  Для этого выполните команду:

  bash
  cp -r /etc/httpd/conf /etc/httpd/conf.bak

- **Обновление Apache**

4 Обновите Apache до последней стабильной версии (рекомендуется 2.4.51 или выше).

Для этого выполните команду:

bash
sudo apt update
sudo apt upgrade apache2

- **Проверка настроек безопасности**

5 Убедитесь, что в конфигурации сервера установлены правильные директивы для защиты от обхода каталога:
text
<Directory "/path/to/document/root">
Require all denied
</Directory>

6 Проверьте наличие и настройку AllowOverride для предотвращения выполнения скриптов из запрещенных директорий.

- **Тестирование после обновления**

7 Перезапустите сервис Apache.

Для этого выполните команду:

bash
sudo systemctl restart apache2

8 Проверьте статус работы сервера:

Для этого выполните команду:

bash
sudo systemctl status apache2

- **Мониторинг и логирование**

9 Настройте мониторинг логов для обнаружения возможных попыток эксплуатации уязвимости:

Для этого выполните команду:

bash
tail -f /var/log/apache2/access.log
tail -f /var/log/apache2/error.log

- **Документация и отчетность**

10 Задокументируйте все выполненные действия и изменения в конфигурации.

11 Подготовьте отчет о выполненных шагах и отправьте его руководству IT.

Дополнительные рекомендации:

- Регулярно проверяйте наличие обновлений для программного обеспечения.
- Рассмотрите возможность внедрения системы обнаружения вторжений (IDS) для мониторинга подозрительной активности на сервере.