# Podatność CVE-2020-1938

CVE-2020-1938 to podatność dotycząca usługi Apache, a konkretnie używania Apache JServ Protocol (AJP). Apache Tomcat posiada zwiększone zaufanie do połączeń z AJP, domyślnie starsze wersje Apache po instalacji posiadały otwarty łącznik AJP, który nie filtrował adresów IP co sprawiało że atakujący mógł korzystać ze zwiększonego poziomu zaufania, co sprawiało że mógł wykonywać akcje niedostępne dla innych typów połączeń np. http.

Szczegóły techniczne:

* Wektor ataku: odczytywanie plików, przesyłanie plików, obejście zabezpieczeń, zdalne wykonanie kodu.
* Dotknięte oprogramowanie: Apache Tomcat 9.0.0.M1-9.0.30, Apache Tomcat 8.5.0-8.5.50, Apache Tomcat 7.0.0-7.0.99
* Opis: Domyślne ustawienia usługi Apache pozwalały atakującemu na obchodzenie zabezpieczeń opartych na IP, autentykacji użytkowników. Pozwalając na dostęp do każdego pliku na serwerze, przesyłanie plików, co daje możliwości na zdalne wykonywanie kodu.

Skutki:

* Możliwość odczytywania plików daje dostęp do wrażliwych danych.
* Przesyłanie plików pozwala na akcje phisingowe, zamianę przekierowań na stronach, wyłudzanie danych, podając się za zaufaną stronę.
* Przesłanie odpowiedniego pliku w teorii może prowadzić do wykonywania zdalnego kodu co daje atakującemu pełny dostęp do serwera.

Rozwiązanie:

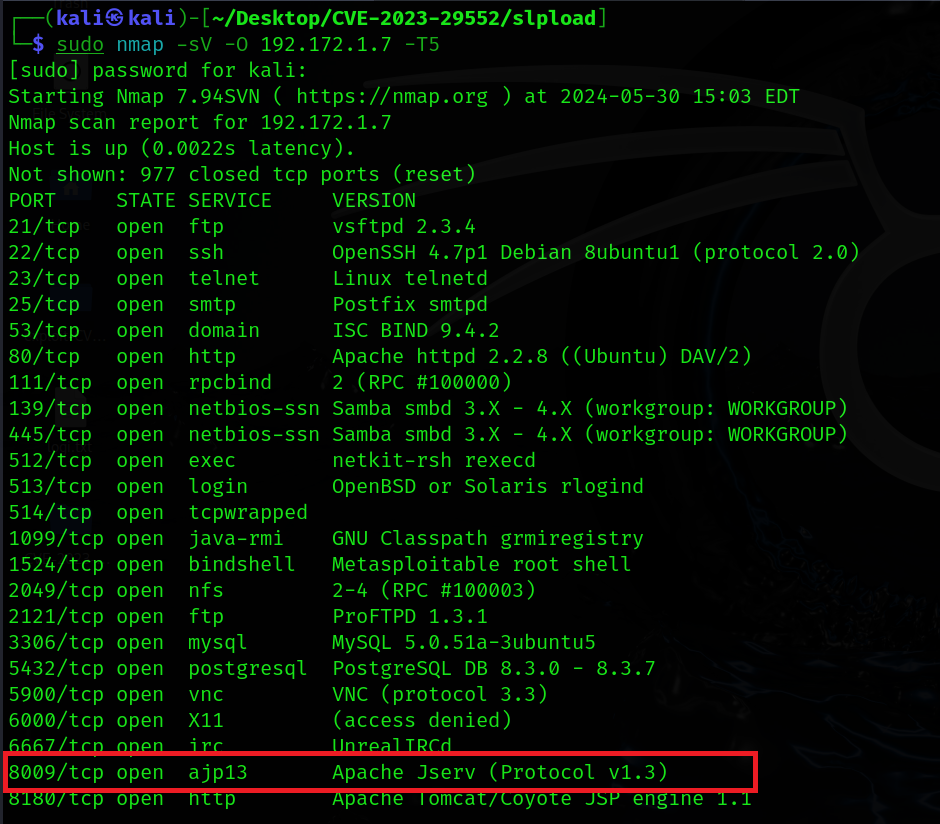
* Zainstalowanie nowszej wersji Apache, zmiana konfiguracji w celu usunięcia dostępu do AJP

## Wstęp

Podatność ta znajduje się na maszynie Metasploitable 2, stworzone zostało zatem środowisko testowe, w którym znajduje się wspomniana wcześniej maszyna wraz z maszyną wirtualną z system operacyjnym Kali Linux.

## Detekcja podatności

Wykrywanie podatności oparte zostało o narzędzie nmap z flagą -sV, celem była maszyna Metasploitable 2, która w środowisku testowym znajduje się pod adresem 192.172.1.7.



Można zauważyć że na porcie 8009 jest dostępna usługa Apache Jserv.

## Symulacja ataku

Korzystając z frameworku metasploit możemy znaleźć odpowiedni moduł pozwalający na wykrycie i wykorzystanie części podatności opowiadającej za czytanie plików. Jako że podatność ta znana jest także jako ,,Ghostcat” wyszukujemy tą fraze

Obraz zawierający zrzut ekranu

Opis wygenerowany automatycznie

Wynik przedstawia ścieżkę do modułu i krótki opis. Następnie następuje przejście do modułu i ustawienie celu, w przygotowanym środowisku Metasploitable 2 znajduje się pod adresem 192.172.1.7.

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Następnie następuje wykonanie modułu i zwrócona zostaje zawartość pliku /WEB-INF/web.xml. Obraz zawierający tekst, zrzut ekranu

Opis wygenerowany automatycznieObraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Po wpisaniu komendy info można zauważyć że ścieżka do pliku również może zostać zmieniona

Mitygacja

Aby usunąć zagrożenie należy usunąć łącznik AJP z pliku konfiguracyjnego serwer.xml, jeśli ta funkcja nadal jest potrzebna możliwie zabezpieczenia to:

- odpowiednia konfiguracja firewalla

- konfiguracja łącznika z atrybutem explicit address aby uniknąć nasłuchiwania na publicznym interfejsie

- ustawienie hasła na łączniku.

Tutaj wykorzystywany jest sposób usunięcia łącznika:

Obraz zawierający tekst, zrzut ekranu, Czcionka, numer

Opis wygenerowany automatycznie

Poprzez usunięcie tej deklaracji łącznik nie jest już otwarty, więc podatność nie może zostać wykorzystana:

Obraz zawierający zrzut ekranu, tekst

Opis wygenerowany automatycznie

Ponowny skan narzędziem nmap potwierdza że udało się zamknąć łącznik:

Obraz zawierający tekst, zrzut ekranu

Opis wygenerowany automatycznie