# Podatność CVE-2014-6271

CVE-2014-6271, znany również jako Shellshock lub Bashdoor, to poważna luka w zabezpieczeniach, odkryta w 2014 roku w powszechnie używanej powłoce Unix, jaką jest Bash. Pozwalała ona atakującym na zdalne wykonanie kodu na podatnych systemach poprzez starannie spreparowane środowisko.

Szczegóły techniczne:

* Wektor ataku: Zdalne wykonanie kodu
* Dotknięte oprogramowanie: GNU Bash w wersji 4.3 i starszych
* Opis: Luka wynikała z sposobu, w jaki Bash przetwarzał pewne specjalnie spreparowane zmienne środowiskowe. Atakujący mogli wykorzystać tę lukę do obejścia ograniczeń środowiska i wykonania dowolnych poleceń powłoki.

Skutki:

* Zdalne przejęcie systemu: Atakujący mogli przejąć pełną kontrolę nad podatnym systemem.
* Kradzież danych: Atakujący mogli ukraść poufne dane, takie jak hasła i dane finansowe.
* Szkodliwe oprogramowanie: Atakujący mogli zainstalować szkodliwe oprogramowanie na podatnym systemie.

Rozwiązanie:

* Aktualizacja Bash do najnowszej wersji

## Detekcja podatności z poziomu konsoli sprawdzanego systemu

Aby sprawdzić czy używany przez nas system posiada tą lukę w zabezpieczeniach należy sprawdzić jaka jest zainstalowana wersja Bash w systemie, można do tego użyć polecenia   
„bash –version”. Jeżeli wersja Bash jest starsza, lub równa wersji 4.3 istnieje duże prawdopodobieństwo, że system jest podatny na tą lukę w zabezpieczeniach. Aby być w stu procentach pewnym należy przeprowadzić kolejny test, tym razem komenda wygląda następująco:

env x='() { :;}; echo vulnerable' bash -c "echo this is a test"

Jeżeli powyższa komenda zwróci jakikolwiek tekst otrzymujemy informację, że system jest podatny w stu procentach i należy zaktualizować Bash do najnowszej możliwej wersji.

## Symulacja ataku

Aby zasymulować atak należy najpierw na komputerze który będziemy atakować stworzyć skrypt który można uruchamiać, będzie on zwracać podstawową stronę internetową. Plik umieszczamy w katalogu /usr/lib/cgi-bin, a plik będzie posiadał nazwę hello.sh

Zawartość pliku hello.sh:

#! /bin/bash

echo "Content-type: text/html"

echo ""

echo "Hello world!"

Należy również zmienić uprawnienia do pliku

sudo chmod 755 hello.sh

Po wejściu na stronę z przeglądarki komputera atakującego otrzymujemy taki widok:  
Obraz zawierający zrzut ekranu, Oprogramowanie multimedialne, oprogramowanie, elektronika

Opis wygenerowany automatycznie

Teraz można przejść do rozpoczęcia ataku na nasz serwer, użyjemy do tego narzędzia Metasploit. Aby uruchomić to narzędzie należy w konsoli wpisać „msfconsole”

Obraz zawierający tekst, zrzut ekranu, diagram

Opis wygenerowany automatycznie

Następnie wyszukujemy w bazie exploity dotyczące shellshock

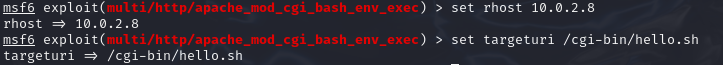
Obraz zawierający tekst, zrzut ekranu, menu, Czcionka

Opis wygenerowany automatycznie

Wybieramy moduł w tym przypadku oznaczony jako numer 1



Następnym krokiem jest ustawienie danych dotyczących atakowanego przez nas urządzenia, czyli adres IP oraz ścieżka do utworzonego wcześniej przez nas skryptu.



Należy również wybrać payload, listę wszystkich dostępnych payload’ów można wyświetlić przy użyciu polecenia „show payloads”. Do tego testu wybieramy payload dotyczący utworzenia połączenia typu „reverse TCP shell”



Po ustawieniu wszystkich informacji można sprawdzić czy wybrane przez nas urządzenia jest podatne na ten atak przy użyciu polecenia „check”



Otrzymaliśmy informację o podatności systemu, więc możemy przejść do wykonywania exploitu

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Jak widać powyżej po udanym ataku otrzymujemy pełny dostęp do konsoli atakowanego komputera z uprawnieniami użytkownika www-data.