# Podatność CVE-2017-7494

CVE-2017-7494 nazywane także ,,SambaCry” opiera się na wykorzystaniu podatności znajdującej się w darmowym oprogramowaniu Samba, które wykorzystuje protokoły sieciowe Server Message Block (SMB)/Common Internet File System(CIFS) aby udostępniać pliki dla wielu klientów Microsoft Windows, może także zintegrowane do Microsoft Windows Server jako kontroler domeny lub członek domeny.

Szczegóły techniczne:

* Wektor ataku: Zdalne wykonanie kodu
* Dotknięte oprogramowanie: Samba w wersjach 3.x późniejszych niż 3.5.0, 4.x przed 4.4.14, 4.5.x przed 4.5.10 i 4.6.x przed 4.6.4
* Opis: Odpowiednia konfiguracja Samby nie ogranicza ścieżki pliku do którego zapisujemy dane jako autoryzowany użytkownik co pozwala na upload plików wykonywalnych na urządzenie korzystające z podatnego oprogramowania.

Skutki:

* Jeśli wyślemy na podatne urządzenie odpowiednio spreparowany plik, będziemy w stanie zdalnie wykonywać na nim polecenia.

Rozwiązanie:

* Zainstalowanie nowszej wersji oprogramowania Samba/ dodatnie do konfiguracji nt pipe support = no

## Wstęp

Stworzenie środowiska testowego okazało się dużym wyzwaniem z powodu braku możliwości instalacji podatnej wersji oprogramowania, jednak na portalu github(<https://github.com/opsxcq/exploit-CVE-2017-7494>) możemy znaleźć dobrze opisany POC z kontenerem dockera z odpowiednią wersją Samby i przygotowaną podatną konfiguracją.

## Detekcja podatności

Aby wykryć podatność możemy użyć narzędzia nmap z flagą -sV, ponieważ do przedstawienia podatności wykorzystywany jest kontener dockera, należy wykonać scan na localhost:

Obraz zawierający tekst, zrzut ekranu

Opis wygenerowany automatycznie

Można zauważyć że na portach 139 i 445 kontenera nasłuchuje Samba w podatnej wersji.

## Symulacja ataku

Wykorzystując dostarczony w [POC](https://github.com/opsxcq/exploit-CVE-2017-7494) atakujemy działający w tle kontener dockera:

Obraz zawierający tekst, zrzut ekranu

Opis wygenerowany automatycznie

Z poziomu kontenera można zobaczyć że w katalogu data znajduje się przesłany payload:

Obraz zawierający tekst, Czcionka, zrzut ekranu, Grafika

Opis wygenerowany automatycznie

Przykładowe zastosowanie

Kradzież danych, najpierw tworzony jest plik z danymi w kontenerze:

Obraz zawierający zrzut ekranu, Czcionka, tekst, Grafika

Opis wygenerowany automatycznie

Następnie przy pomocy wykorzystanej podatności mamy do nich dostęp.

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Jest to oczywiście tylko przykład, mając możliwość wykonania każdej komendy atakujący może zrobić o wiele więcej np. zaszyfrować dane i wykorzystać to do ataku ransomware.