CVE-2022-32250-exploit

OPIS

Ta podatność umożliwia lokalnemu użytkownikowi, który ma zdolność tworzenia przestrzeni nazw użytkownika/sieci, eskalację swoich uprawnień do poziomu roota. Problem wynika z nieprawidłowej kontroli NFT_STATEFUL_EXPR, co prowadzi do błędu typu use-after-free.

Wersje objęte podatnością:

- Ubuntu <= 22.04 przed łatą bezpieczeństwa
    - Linux ubuntu 5.15.0-27-generic

Głównym skutkiem tej luki jest uzyskanie przez osobę atakującą uprawnień roota w systemie docelowym.

Testy podatności:

Testy podatności próbowano przeprowadzić na ubuntu 22.04 z wersją kernela Linux ubuntu 5.15.0-27-generic.

Po zainstalowaniu systemu okazało się, że występują problemy z działaniem systemu.

Maszyna wirtualna była nieobsługiwalna– nie otwierał się terminal.

Teoretyczny opis działania:

Plik z exploitem należałoby pobrać, a następnei skompilować za pomocą komendy *gcc exp.c -o exp -l mnl -l nftnl -w*, a następnie uruchomić *komendą* ./exp.

Exploit składa się z pięciu etapów

Etap 0:

W tym etapie tworzona są tablice oraz zestawy przy użyciu interfejsu Netlink. Każda tabela i zestaw są przypisywane do protokołu IPv4.

Etap 1:

W etapie 1 celem jest uzyskanie wycieku adresu w pamięci heap (sterta) poprzez manipulacje kluczami w systemie Linux.

Dla każdej pary tabela-zestaw tworzona jest struktura przechowująca odpowiednie nazwy. Funkcja spray_keyring tworzy dużą liczbę kluczy, co może powodować fragmentację pamięci i doprowadzić system do uzyskania wycieku adresu heap.

Etap 2:

Celem etapu 2 jest uzyskanie adresu KASLR (Kernel Address Space Layout Randomization). KASLR to technika bezpieczeństwa, która losowo rozmieszcza przestrzeń adresową jądra systemu operacyjnego

w celu utrudnienia ataków opartych na znanym układzie pamięci. Do tego celu wykorzystywane są operacje związane z io_uring oraz kolejkami komunikatów.

Etap 3:

Na tym etapie, celem jest nadpisanie ścieżki do pliku modprobe i wykonanie złośliwego kodu. Po uzyskaniu adresu KASLR z poprzedniego etapu, nadpisywana jest ścieżka modprobe_path w pamięci jądra, co pozwala na wykonanie złośliwego pliku z uprawnieniami roota. Następnie uruchamiany jest plik dummy lub shell w celu uzyskania uprawnień roota.

Mitygacja podatności

Możliwym sposobem na naprawę luki jest aktualizacja jądra systemu do wersji po patchu: 520778042ccca019f3ffa136dd0ca565c486cedd (26 May, 2022).