**Użytkownicy Linuksa bezpieczniejsi dzięki zabezpieczeniu Check Pointa**

**Badacze z firmy Check Point przedstawili nowy mechanizm zabezpieczenia dla użytkowników Linuksa o nazwie „bezpieczne łączenie” (ang. Safe-linking). Przez prawie dwie dekady hakerzy wykorzystywali projekt zarządzania pamięcią w programie Linux, aby przejąć kontrolę nad komputerem docelowym. Teraz mechanizm Check Pointa znacznie utrudni cyberprzestępcom życie.**

Przez dwadzieścia lat programy Linuksa były narażone na ataki polegające na uszkodzeniu pamięci, w których haker wprowadzał złośliwy kod po zmianie lub modyfikacji pamięci w systemie komputerowym. Pierwotna konstrukcja mechanizmu pamięci pochodzi z 2000 r. Już pięć lat później starano się wprowadzić ochronę o nazwie *Bezpieczne rozłączanie,* jednak dotyczyła ona tylko jednej części projektu. Badacze z Check Pointa w końcu znaleźli sposób na ochronę pozostałych części.

Chcąc położyć kres temu długotrwałemu problemowi, programiści Check Point stworzyli nowy mechanizm bezpieczeństwa „bezpieczne łączenie” (safe-linking), który ma chronić wewnętrzną strukturę przed włamaniem. Wykorzystuje on tzw. mechanizm losowej zmiany adresów, który jest obecnie stosowany w większości nowoczesnych systemów operacyjnych, zwanym Address-Space-Layout-Randomization (ASLR). ASLR losowo wybiera adres bazowy, na który program zostanie załadowany, utrudniając przestępcom możliwość skutecznego włamania.

Mówiąc prościej, „Safe-Linking” usuwa dane adresowe programu, więc haker nie może już mieć pewności, gdzie w pamięci systemu zostanie on załadowany - co znacznie utrudnia mu uruchomienie exploita przeciwko programowi.

- *Podczas gdy deweloperzy exploitów znają ten problem od wielu lat, programiści bibliotek nie byli świadomi problemu - stąd nic przez lata nie zostało naprawione. Przekazując programistom opinie oraz pomysł na naprawę, udało nam się raz na zawsze rozwiązać ten problem. Użytkownicy Linuksa powinni być świadomi tej aktualizacji i upewnić się, że po jej opublikowaniu przejdą do korzystania z najnowszej wersji standardowej biblioteki* – mówi Eyal Itkin z Check Pointa

Analitycy mają nadzieję, że rozwiązanie pozwoli na zablokowanie kilku głównych exploitów, które badane były przez ekspertów bezpieczeństwa przez lata. Podejście Safe-Linking zostało wdrożone i z powodzeniem zintegrowane z najważniejszymi środowiskami systemowymi i głównymi bibliotekami w systemie operacyjnym Linux.

Więcej informacji o projekcie dostępnych jest na [blogu Check Point Research](https://research.checkpoint.com/2020/safe-linking-eliminating-a-20-year-old-malloc-exploit-primitive/).