Niezabezpieczające zabezpieczenia

22 stycznia 2011

Twórca projektu grsecurity, Brad Spengler, ostrzega, że większość z zastosowanych w Linuksie mechanizmów kontroli uprawnień może zostać wykorzystana przez napastnika do przełamania zabezpieczeń systemu. Filozofia bezpieczeństwa w Linuksie opiera się w olbrzymiej mierze na ścisłej kontroli dostępu do usług, procesów i zasobów. Z jednej strony pozwala to ograniczyć uprawnienia poszczególnych użytkowników do rzeczywiście potrzebnych im do pracy, a z drugiej – w przypadku ataku zmniejsza rozmiary szkód, gdyż np. narzędzie, które udało się wykorzystać napastnikowi do konkretnych działań, nie będzie miało uprawnień do wykonania innych komend lub uzyskania dostępu innych zasobów.

Spengler przetestował 35 linuksowych mechanizmów pod kątem wykorzystania ich podczas przeprowadzanego ataku. Odkrył, że 21 z nich może pozwolić napastnikowi na zwiększenie uprawnień w systemie lub inny sposób nim manipulować.

Jednym z takich mechanizmów jest CAP_SYS_ADMIN, który umożliwia podmontowywanie i odmontowywanie systemu plików. Potencjalnie pozwala on napastnikowi na podmontowanie własnego systemu plików nad istniejącym i zastąpienie zainstalowanych programów dowolnym kodem. Spengler mówi, że za pomocą CAP_SYS_ADMIN można też przekierowywać pakiety na firewallu, a zatem napastnik ma możliwość przekierowania połączeń sshd na dowolny serwer i kradzież haseł oraz nazw użytkownika, co pozwoli na logowanie się do systemu na prawach administratora.

Praca Spenglera nie oznacza, że Linux jest systemem szczególnie niebezpiecznym. Większość opisanych przez niego scenariuszy ataków jest możliwa do przeprowadzenia jedynie w bardzo specyficznych warunkach lub też wymaga fizycznego

dostępu do atakowanego systemu.

Autor: Mariusz Błoński
Na podstawie: Heise
Źródło: Kopalnia Wiedzy