**Luka w systemie logowania zagraża firmom i użytkownikom na całym świecie! Blisko 1/3 firm doświadczyła próby jej wykorzystania.**

**9 grudnia zgłoszono poważną lukę w zabezpieczeniach zdalnego wykonania kodu (RCE) w pakiecie logowania Apache Log4j 2 w wersjach 2.14.1 i niższych, będącą najpopularniejszą biblioteką logowania Java z ponad 400 000 pobrań. Pakiet jest powszechnie wykorzystywany, umożliwiając logowanie m.in. do popularnych aplikacji. Jak informują specjaliści z Check Point do sobotniego wieczora lukę próbowano wykorzystać w ponad 31,5 proc. sieci korporacyjnych na całym świecie! Aktywność cyberprzestępców była widoczna również w Polsce.**

Eksperci z Check Point Research uważnie monitorują masowe próby skanowania i wykorzystania ogłoszonych 9 grudnia eksploitów Apache Log4j (CVE-2021-44228). Ich zdaniem, obecnie złośliwą aktywność wykazują głownie „skanerzy” oraz cyberprzestępcy zajmujący się wydobywaniem kryptowalut, jednak za kulisami obecnych wydarzeń mogą stać hakerzy o bardziej niecnych celach.

Eksperci są zgodni, że jest to niewątpliwie jedna z najpoważniejszych luk w zabezpieczeniach internetowych w ostatnich latach.

**Logowanie na celowniku hakerów**

Apache Log4j jest najpopularniejszą biblioteką logowania Java z ponad 400 000 pobrań z jej projektu na GitHubie. Jest wykorzystywana przez niezliczoną liczbę firm na całym świecie, umożliwiając logowanie w szerokim zestawie popularnych aplikacji. Wykorzystanie luki jest – zdaniem specjalistów - relatywnie proste i pozwala na przejęcie kontroli nad serwerami internetowymi opartymi na Javie oraz przeprowadzenie ataku zdalnego wykonania kodu. Do tej pory próbowano wykorzystać exploita w ponad 31,5% sieci korporacyjnych na całym świecie.

Firma Check Point Software wydała już nową ochronę Quantum Gateway opartą na Threat Cloud, która zapobiega temu atakowi. Od jej wdrożenia zapobiegła co najmniej 470 000 prób przydzielenia luki. Ponad 45% tych prób zostało wykonanych przez znane szkodliwe grupy. Część prób naruszeń wykryto również wśród polskich przedsiębiorstw.