Aktualizacja w związku z Apache Log4j CVE-2021-44228

Grupa OASIS wraz z dostawcami usług IT na całym świecie aktywnie zareagowała na ostatnio zgłoszoną lukę w zabezpieczeniach zdalnego wykonania kodu (RCE) w bibliotece Apache Log4j Java.

Luka, która została upubliczniona 9 grudnia 2021 r., została sklasyfikowana z wynikiem CVSS wynoszącym 10,0. Oznacza to, że zagrożenie zostało ocenione jako krytyczne.

Steve Townley, CIO w OASIS Group, zapewnił: „Podjęliśmy natychmiastowe działania w celu wykrycia wszelkich powiązanych zagrożeń i złagodzenia konsekwencji powstania luki w CVE-2021-44228. Chcielibyśmy zapewnić naszych klientów, że nie znaleźliśmy żadnego aktywnego wykorzystania tej luki w naszych systemach."

Apache Software wydało uaktualnienie do Log4j 2.15.0, aby załatać tę lukę, a tam, gdzie to było konieczne, zostało to zaimplementowane w systemach grupy OASIS.

„Ponieważ OASIS opracowuje nasz pakiet Omnidox Suite, byliśmy w stanie natychmiast wdrożyć aktualizację Log4j 2.15.0, a także dodać dodatkowe konfiguracje Java jako dodatkowy poziom bezpieczeństwa". Kontnuuje Steve Townley.

Jakie działania muszą podjąć klienci OASIS?

Dla klientów korzystających z systemów OASIS nie są wymagane żadne działania, dokonaliśmy już niezbędnych aktualizacji i nadal monitorujemy pod kątem zagrożeń, tak jak zawsze. Jak wspomniano powyżej, Log4j jest szeroko stosowany w wielu aplikacjach IT i zalecamy skontaktowanie się z wewnętrznym działem IT lub innymi dostawcami.

Kilka innych przydatnych informacji:

Co to jest wynik CVSS?

CVSS to skrót od Common Vulnerability Scoring System. Jest to standard branżowy, który podaje liczbową reprezentację (0-10, 120 oznacza najwyższą) zagrożenia daną luką w zabezpieczeniach oprogramowania.

Co to jest zdalne wykonanie kodu?

Zdalne wykonanie kodu (RCE) to cyberatak, który umożliwia atakującemu zdalny dostęp do cudzego urządzenia lub systemu i kontrolowanie go bez konieczności podawania nazwy użytkownika lub hasła. Można to zrobić zdalnie z dowolnego miejsca na świecie.

Co to jest Log4j?

Prawie całe oprogramowanie prowadzi rejestr błędów i innych ważnych zdarzeń. Log4j to jeden z najpopularniejszych pakietów logowania używanych na całym świecie.

W jaki sposób OASIS złagodził tę lukę?

O podatności został zaalarmowany zespół wewnętrznych specjalistów IT OASIS, w tym między innymi inżynierowie oprogramowania IT i specjaliści ds. bezpieczeństwa infrastruktury IT. Zespoły natychmiast pracowały nad aktualizacją, w razie potrzeby, Log4j do wersji 2.15.0, która została wydana jako adres CVE-2021-44228.

Tam, gdzie to możliwe, dodaliśmy również dodatkowe konfiguracje Java i wzmocniliśmy zabezpieczenia za pośrednictwem naszych firewalls i innego oprogramowania zabezpieczającego.