# Informacje na temat wpływu podatności wykrytej w komponencie Apache Log4j2 (CVE-2021-44228) na oprogramowanie AVEVA

*Aktualizacja 21-12-2021*

Produkty AVEVA nie są dotknięte podatnością Log4j2 za wyjątkiem następujących komponentów:

- AVEVA Historian – wersje od 2017 do 2017 Update 3 SP1 P01 zawierają podatne komponenty jako składniki usługi Elastic Search. Komponent ten zawiera podatną wersję Log4j2 natomiast analiza zagrożenia wykazała, że nie istnieje ścieżka przez którą użytkownik może użyć komponentu Elastic Search (używającego Log4j2) do przetwarzania przesłanych przez niego danych. To oznacza ograniczenie potencjalnego ryzyka ataku. Skanery systemów bezpieczeństwa mogą wykrywać Log4j w folderach produktów AVEVA natomiast konfiguracja w jakiej Log4j jest używany w Elastic Search nie jest podatna. Dla użytkowników Historiana AVEVA zaleca następujące kroki:
  - W aplikacjach w których użytkownicy nie korzystają z komponentu **Historian Client Web** (InSight) zalecane jest zatrzymanie i wyłączenie (disable) usługi „Wonderware Historian Search", która korzysta z Elastic Search a przez to z Log4j
  - W pozostałych aplikacjach zalecane jest wykonanie kroków wskazanych przez dostawcę komponentu Elastic search :

    ESA-2021-31 - Elastic Security Announcement regarding, Apache Log4j2 CVE-2021-4428: Apache Log4j2 Remote Code Execution (RCE) Vulnerability - CVE-2021-44228 - ESA-2021-31 - Announcements / Security Announcements - Discuss the Elastic Stack

    Opcjonalnie można skorzystać z poniższego skryptu aby zastosować poprawkę konfiguracyjną automatycznie. Aby to zrobić należy uruchomić PowerShell ISE jako administrator a następnie wkleić i uruchomić następujący skrypt:

    TA000032828_ISEScript.zip

- AVEVA BI Gateway – w przypadku tego produktu należy wdrożyć następującą rekomendację https://kb.tableau.com/articles/issue/Apache-Log4j2-vulnerability-Log4shell

Firma AVEVA kontynuuje prace nad kolejnymi zaleceniami i poprawkami ograniczającymi ryzyko. Będziemy umieszczać je w kolejnych aktualizacjach tego informatora.

Dodatkowe źródła informacji na temat Log4j:

AVEVA Statement on the Apache Log4j vulnerably CVE-2021-44228: AVEVA Statement on the Apache Log4j vulnerability CVE-2021-44228

Apache Log4j Vulnerability Guidance: https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance

ESA-2021-31 - Elastic Security Announcement regarding, Apache Log4j2 CVE-2021-4428: Apache Log4j2 Remote Code Execution (RCE) Vulnerability - CVE-2021-44228 - ESA-2021-31 - Announcements / Security Announcements - Discuss the Elastic Stack