Technical Alert 004

Vulnerabilità Apache Log4j CVE-2021-44228

Rev 6 - 07/01/2022

Technical Services

Problema

Quali prodotti AVEVA sono interessati dalla vulnerabilità critica "Log4Shell" in Apache Log4j, CVE-2021-44228

NOTA: Le indicazioni seguenti si applicano anche alle vulnerabilità Log4j aggiuntive CVE-2021-45046 e CVE-2021-45105.

Soluzione

I prodotti AVEVA non sono interessati da Apache Log4j, ad eccezione di quanto descritto di seguito:

Vulnerabile

- Le versioni di AVEVA Historian da 2017 a 2017 Update 3 SP1 P01 sono interessate dalla dipendenza dalle versioni vulnerabili di Elasticsearch. AVEVA non ha trovato alcun percorso per l'elaborazione dell'input dell'utente da parte del componente Elasticsearch utilizzando Log4j vulnerabile, il che suggerisce una priorità inferiore durante la pianificazione delle azioni difensive.

  AVEVA suggerisce una delle due strategie di mitigazione:

  - Gli ambienti che non utilizzano Historian Insight (da allora ribattezzato **Historian Client Web**) possono utilizzare la console di gestione dei servizi Windows per disabilitare Elasticsearch incorporato arrestando e disabilitando il servizio "**Wonderware Historian Search**".

  - Aggiornare Apache Log4j alla versione 2.17.1 utilizzando le istruzioni presenti nel file zip allegato (TA000032828 Readme Historian Log4j Patch).

- AVEVA Net Workhub e Dashboard on premise versioni 5.1.5 e precedenti sono interessati dalla dipendenza da versioni vulnerabili di Accusoft PrizmDoc. AVEVA consiglia vivamente di eseguire l'aggiornamento a una versione di AVEVA Net Workhub and Dashboard con supporto mainstream o esteso.

Mitigato

- Le versioni 2020 di AVEVA Historian e successive non sono interessate dalla dipendenza dalle versioni mitigate di Elasticsearch.
  Vedere l'annuncio di sicurezza "ESA-2021-31 - Annuncio sulla sicurezza riguardante Apache Log4j2 CVE-2021-4428" nella sezione 'Riferimenti esterni' di seguito.
  Facoltativamente, aggiornare Apache Log4j alla versione 2.17.1 utilizzando le istruzioni nel file zip allegato (TA000032828 Readme Historian Log4j Patch).
- Le offerte cloud di AVEVA Net Workhub e Dashboard, nonché le versioni locali 5.1.6 e successive non sono interessate dalla dipendenza dalle versioni mitigate del visualizzatore Accusoft PrizmDoc.

- La dipendenza di AVEVA BI Gateway da Tableau Server può essere mitigata in base alle indicazioni di Salesforce nella sezione 'Riferimenti esterni' di seguito.

NOTA: gli scanner di sicurezza potrebbero rilevare Log4j nelle offerte di prodotti AVEVA di cui sopra, anche se la configurazione non è vulnerabile.

Indagine in Corso

- L'indagine sui prodotti AVEVA non inclusi nel supporto principale o esteso farà leva sui risultati riportati dalla comunità e sarà periodicamente incorporata in questo avviso tecnico. CVE-2021-44228 è stato introdotto nel codebase Apache Log4j nel 2013.

Circostanza speciale

- AVEVA Historian 2014 R2 SP1 P02 e tutti i precedenti non sono interessati a causa della dipendenza dalle versioni di Elasticsearch precedenti a CVE-2021-44228; Tuttavia, queste versioni di Elastic non sono più supportate da Apache. AVEVA consiglia vivamente di eseguire l'aggiornamento a una versione di AVEVA Historian con supporto mainstream o esteso.

AVEVA sta sviluppando linee guida e/o piani per gli aggiornamenti di sicurezza per affrontare i problemi di dipendenza dei sottocomponenti relativi ad Apache Log4j.

AVEVA continua a indagare sui sottocomponenti potenzialmente interessati nella catena di fornitura per offerte di prodotti AVEVA, integrazioni di partner e siti Web correlati.

AVEVA consiglia ai clienti di implementare misure difensive provvisorie in conformità con le raccomandazioni CISA riportate di seguito per contrastare la vulnerabilità di Log4j.

INFORMAZIONI AGGIUNTIVE

Questo articolo riguarda tutti i prodotti AVEVA e verrà aggiornato se necessario.

Per il download del seguente documeto in lingua inglese, fare riferimento a questo link TA000032828

Riferimento:

- Indagine CR-125798 e notifica AVEVA originale: AVEVA Statement on the Apache Log4j vulnerably CVE-2021-44228

Riferimenti esterni

- Linee guida generali della Cyber Security Infrastructure Security Agency (CISA): Apache Log4j Vulnerability Guidance
- Mitigazioni di Tableau per le versioni esistenti: https://kb.tableau.com/articles/issue/Apache-Log4j2-vulnerability-Log4shell
- ESA-2021-31 - Annuncio sulla sicurezza riguardante 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
- Annuncio di Accusoft sull'impatto di Log4j su PrizmDoc: https://www.accusoft.com/support/apache-log4j-vulnerability/

Autore: Ambra Spenga

Disclaimer

Il presente documento è fornito a scopo di esempio e non sostituisce la documentazione AVEVA. L'applicazione di quanto contenuto, in un preciso ambito applicativo, deve essere sempre validata da un tecnico Wonderware. La documentazione rilasciata da AVEVA resta il riferimento tecnico ufficiale da seguire: softwaresupport.aveva.com. Wonderware Italia non si assume la responsabilità di un'applicazione scorretta di questo documento.