

# **Informazioni aggiuntive urgenti sulla falla del sistema Apache**

*Un gruppo di specialisti di sicurezza informatica ha esaminato la vulnerabilità critica, che è stata pubblicata il 9 dicembre 2021, relativa al sistema Apache Log4j Java.*

Gli organi tecnici di comunicazione, afferenti ai sistemi informatici, hanno dato notizia della falla presente in un diffusissimo sistema informatico. Anche questo bollettino ne ha dato notizia ed aggiungiamo, per i nostri lettori, ulteriori indicazioni sulla possibilità di mettere sotto controllo questa falla relativa al sistema Apache Log4j Java.

Pubblicità

<#? QUI-PUBBLICITA-SCORM1-[EL0143] ?#>

Ecco le raccomandazioni che sono state pubblicate, per mettere sotto controllo questa pericolosa vulnerabilità.

- Effettuate subito una rassegna di tutti i sistemi che utilizzano Apache Log4j Java, ed effettuate tutti gli appropriati aggiornamenti.
- Aggiornate immediatamente tutte le versioni alla edizione 2.15.0.
- Per i sistemi che non possono essere immediatamente migliorati, identificate rimedi alternativi come ad esempio il sandboxing, air gapping o addirittura disconnettendo il sistema dalla rete Internet. Apache ha pubblicato una guida, che aiuta a mettere sotto controllo questa vulnerabilità, per sistemi che non possono essere immediatamente aggiornati. Questa guida si trova all'indirizzo Web <https://logging.apache.org/log4j/2.x/security.html>
- Conservate copia di evidenze di natura criminologica, se possibile, prima di intervenire sul sistema,
- Confermate che il vostro centro di gestione della sicurezza tiene sotto controllo i sistemi interfacciati con il mondo esterno, per individuare tempestivamente possibili compromissioni,
- Aggiornate i firewall e altri strumenti di interfaccia per impedire connessioni verso l'esterno di sistemi che utilizzano Log4j. Sono già disponibili numerosi elenchi di indirizzi IP che tengono sotto controllo questa vulnerabilità ed è quindi opportuno inserire questi indirizzi in una lista bloccata,
- Accertatevi che il vostro sistema di registrazione dei collegamenti di rete tenga sotto controllo ogni collegamento a una libreria che utilizza Apache Log4j Java,
- Controllate che i vostri fornitori di servizi informatici ed i loro sistemi e prodotti siano stati aggiornati o abbiano comunque messo sotto controllo questa vulnerabilità,
- Riesaminate il vostro piano di messa sotto controllo di incidenti informatici e prendete in specifica considerazione lo scenario connesso a questa vulnerabilità. Accertatevi che tutti i contatti con la squadra di emergenza siano aggiornati.
- Se la vostra azienda è coinvolta in un'acquisizione di altre aziende, verificate i piani di sicurezza che sono stati già adottati dalla azienda, che intendete acquisire.



Licenza [Creative Commons](#)

---

[www.puntosicuro.it](http://www.puntosicuro.it)