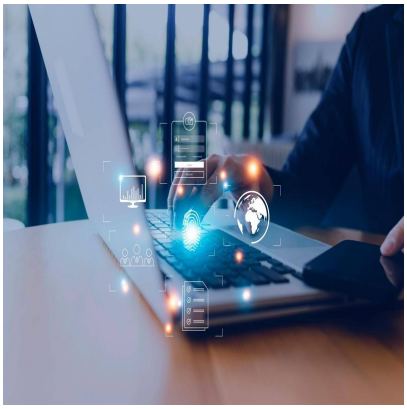


Cybersicurezza, agenzia Usa: â??Alert su vulnerabilitÃ Javaâ?•

Descrizione

default watermark

(Adnkronos) â?? La Cybersecurity and Infrastructure Security Agency (Cisa) americana ha invitato le aziende e le organizzazioni ad aggiornare tutti i sistemi basati su Java. Il linguaggio di programmazione targato Oracle (che ha rilasciato una patch ma non ha commentato la vicenda), oltre a essere molto diffuso su Internet, Ã¨ ampiamente utilizzato da compagnie aeree, banche, ospedali ed enti governativi.

Secondo lâ??agenzia, che conferma quanto scoperto dalla startup Calif attraverso lâ??uso dellâ??Ai per individuare le vulnerabilitÃ del linguaggio di programmazione, la falla scoperta espone Java ad attacchi informatici anche molto gravi. Il linguaggio Ã¨ utilizzato dal 90% delle societÃ Fortune 500. Lâ??allarme riguarda la potenziale interruzione di servizi web. Sul sito dellâ??agenzia si legge che â??la CISA raccomanda vivamente alle organizzazioni di applicare immediatamente la patch per la vulnerabilitÃ CVE-2026-114938 di Oracle Java, recentemente scoperta. Questa vulnerabilitÃ critica di corruzione della memoria, nota come â??Java4Shellâ?•, interessa il decodificatore Base64 della Java Virtual Machineâ?•. Lo sfruttamento della falla potrebbe â??consentire lâ??esecuzione di codice remoto senza autenticazioneâ?•. I ricercatori di Calif hanno dimostrato di poter corrompere i dati Java ottenendo pieno accesso non autorizzato al sistema sottostante.

Un allarme molto simile a quello lanciato dopo che OpenAi ha rivelato le vulnerabilitÃ di Php, un altro dei linguaggi di programmazione piÃ¹ utilizzati sul web, che ha provocato unâ??allerta internazionale arrivata anche in Italia, dove lâ??Acn ha identificato 285.149 siti vulnerabili. Il New York Times ha anche ipotizzato che la vulnerabilitÃ potesse essere alla base di incidenti recenti come quello della Nsa, che stanno gettando ombra sul perimetro di sicurezza cibernetica americano.

â??

economia

webinfo@adnkronos.com (Web Info)

Categoria

1. Comunicati

Tag

1. Ultimora

Data di creazione
Novembre 18, 2026
Autore
redazione

default watermark