Vulnerabilità della sicurezza in Apache Tomcat CVE-2025-24813, CVE-2024-50379, CVE-2025-31651

Technical Alert 012 - REV.4

29/08/2025

PROBLEMA

Quali prodotti **AVEVA** sono interessati dalla vulnerabilità critica in Apache Tomcat:

- CVE-2025-24813
- CVE-2024-50379
- CVE-2025-31651

SOLUZIONE

Per **CVE-2025-24813** e **CVE-2024-50379**:

Le offerte di prodotti AVEVA non sono interessate dalla vulnerabilità Apache Tomcat. La giustificazione dello stato non interessato è dovuta al fatto che le scritture sono disabilitate. Apache segnala che le scritture devono essere abilitate affinché il servlet predefinito esponga questa vulnerabilità.

Per **CVE-2025-31651**:

Le offerte di prodotti AVEVA non sono interessate dalla vulnerabilità Apache Tomcat. La giustificazione dello stato non interessato è dovuta al fatto che le regole di riscrittura sono disabilitate. Apache segnala che le regole di riscrittura devono essere abilitate affinché il servlet predefinito esponga questa vulnerabilità.

NOTA: Gli scanner di sicurezza potrebbero rilevare la vulnerabilità di Apache Tomcat CVE-2025-24813, CVE-2024-50379 o CVE-2025-31651 sui computer in cui è installato AVEVA Enterprise License Server Legacy Support. I rilevamenti di CVE-2025-24813 associati ai componenti installati dai prodotti elencati nell'Appendice possono essere ignorati con lo stato VEX di *Vulnerable_code_not_in_execute_path*.

MISURE DIFENSIVE e CONSIDERAZIONI GENERALI

AVEVA Enterprise License Server eredita le dipendenze di Apache Tomcat da un componente di terze parti. Di conseguenza, supportiamo solo le versioni di Apache Tomcat fornite dal nostro fornitore. Eventuali modifiche o aggiornamenti oltre a queste versioni non sono ufficialmente supportati, poiché il loro impatto non può essere garantito.

AVEVA consiglia ai clienti di applicare approcci generali di difesa in profondità per proteggere i loro ambienti. Riferimento:

Pubblicazione speciale NIST 800-82r3: Guida alla sicurezza della tecnologia operativa (OT)

INFORMAZIONI AGGIUNTIVE

L'analisi di questo articolo riguarda tutti i prodotti **AVEVA** e verrà aggiornata se necessario.

NOTA: AVEVA prevede di affrontare i rilevamenti del NESSUS plugin 12085 nelle versioni future dei prodotti AVEVA interessati.

Appendice:

Prodotti che forniscono AVEVA Enterprise License Server

- System Platform
- Application Server
- Historian
- Historian Client
- InTouch
- System Monitor
- AVEVA Edge
- AVEVA Reports for Operations
- AVEVA Communication Drivers Pack
- Batch Management
- MES
- Mobile Operator
- Plant SCADA
- Recipe Manager
- Work Tasks

Riferimenti esterni:

- https://nvd.nist.gov/vuln/detail/CVE-2025-24813
- https://nvd.nist.gov/vuln/detail/CVE-2024-50379
- https://nvd.nist.gov/vuln/detail/CVE-2025-31651
- https://lists.apache.org/thread/j5fkjv2k477os90nczf2v9l61fb0kkgq
- https://www.rapid7.com/blog/post/2025/03/19/etr-apache-tomcat-cve-2025-24813-what-you-need-to-know/