

Nessus scan identified the Apache Log4j vulnerability CVE-2026-49844 in the DWS component

000045950 | General Info | Last updated 2026-09-09 | ControlSuite, ControlSuite AutoStore, ControlSuite Equitrac, ControlSuite Shared Components

Issue

A Nessus scan identified the Apache Log4j vulnerability, CVE-2026-49844, in the DWS component.

Solution

The Tungsten Development team has reviewed CVE-2026-49844 and confirmed DWS is not affected by the vulnerability. About the log4j version, the Tungsten development team has created a fix to upgrade log4j to 2.26.1. The following libraries are now upgraded to version 2.26.1 to resolve the issue:

- log4j-core-2.17.2.jar
- log4j-api-2.17.2.jar
- log4j-1.2-api-2.17.2.jar

Applies to

Product	Version
Control Suite	CS 1.5.2

References

ControlSuite Vulnerability Overview

<https://aio-eus-uat-cae-aif-app14-local.redglacier-35d7ee4f.eastus.azurecontainerapps.io/article/45950>