

ShareScan CVE-2026-65637

000046016 | How To | Last updated 2026-09-16 | ShareScan

Issue

A vulnerability scan (Qualys QID 735213) reports [CVE-2026-65637](#) against the Apache Tomcat 9.0 instance installed with eCopy ShareScan. The finding is rated **Moderate** by the Apache Software Foundation and **Medium** by Qualys, and it is raised on any ShareScan server running Apache Tomcat 9.0.115 through 9.0.120.

Customers and auditors ask whether eCopy ShareScan is exposed to this virtual host access bypass and what remediation is required.

Cause

CVE-2026-65637 is an incomplete fix for CVE-2026-32990. It allows **HTTP/2** requests that use the no-authority pseudo-header to bypass strict SNI (Server Name Indication) hostname validation. By exploiting the mismatch between SNI and HTTP host validation, an attacker could reach virtual hosts they should not have access to.

- Affected Apache Tomcat versions: 9.0.115 - 9.0.120
- Fixed in Apache Tomcat: 9.0.121

The vulnerability has two prerequisites: HTTP/2 must be enabled, and strict SNI validation must be configured in a multi virtual host setup.

Solution

eCopy ShareScan is not affected by CVE-2026-65637. No action is required.

Neither prerequisite applies to the product:

- **HTTP/2 is not enabled.** All active Connectors in the eCopy ShareScan server.xml use `protocol="HTTP/1.1"`. HTTP/2 support (`Http2Protocol`) is disabled across all shipped versions (6.5, 2025.3, 2026.3). Without HTTP/2 the no-authority bypass mechanism cannot be triggered.
- **Strict SNI validation is not configured.** Even if HTTP/2 were present, the attack requires a specific multi virtual host setup with strict SNI enforcement, which is not part of the eCopy ShareScan configuration.

Optional: if your security policy requires the scanner finding to be cleared rather than documented as not applicable, Apache Tomcat can be updated manually to version 9.0.121. Follow the *Manual update of Apache Tomcat* article below, and confirm the target version against *ShareScan: Apache Tomcat version requirements* before updating. This is a hardening step to satisfy the scanner, not a fix required for product security.

Applies to

Product	Version	Build	Environment	Hardware
Kofax eCopy ShareScan	v6.5 - v6.6			
Tunsten eCopy ShareScan	v6.7 - v2026.3			

Request created:

2026-09-16

References

- Manual update of Apache Tomcat
- ShareScan: Apache Tomcat version requirements
- ShareScan: Java requirements
- eCopy ShareScan: Removing Java / ApacheTomcat
- ShareScan Vulnerability overview

<https://aio-eus-uat-cae-aif-app14-local.redglacier-35d7ee4f.eastus.azurecontainerapps.io/article/46016>