

ShareScan CVE-2026-68569

000046018 | How To | Last updated 2026-09-16 | ShareScan

Issue

A vulnerability scan (Qualys QID 735215) reports [CVE-2026-68569](#) against the Apache Tomcat 9.0 instance installed with eCopy ShareScan. The finding is rated **Important** by the Apache Software Foundation and **Critical** by Qualys, and it is raised on any ShareScan server running Apache Tomcat 9.0.0-M1 through 9.0.120.

Customers and auditors ask whether eCopy ShareScan is exposed to this authentication fail open condition and what remediation is required.

Cause

CVE-2026-68569 is a fail open condition in Apache Tomcat's principal lookup. With certain authentication methods (CLIENT-CERT and SPNEGO), a user could be successfully authenticated by Tomcat even if that user did not exist in the configured `DataSourceRealm` or `JDBCRealm`, which could grant unauthorized access to protected resources.

- Affected Apache Tomcat versions: 9.0.0-M1 - 9.0.120
- Fixed in Apache Tomcat: 9.0.121

Exploitation requires both an affected Realm type and an affected authentication method.

Solution

eCopy ShareScan is not affected by CVE-2026-68569. No action is required.

Neither prerequisite is present in the product:

- **Realm type.** The vulnerability only manifests with `DataSourceRealm` or `JDBCRealm`. All eCopy ShareScan versions (6.5, 2025.3, 2026.3) exclusively use `UserDatabaseRealm` nested inside `LockOutRealm`. These Realm types are not subject to the faulty principal lookup logic.
- **Authentication method.** The vulnerability is triggered by CLIENT-CERT or SPNEGO authentication. No `<login-config>` or `<auth-method>` declarations using these methods exist in any `web.xml` across the product.

Because both prerequisites are absent, the attack vector described in CVE-2026-68569 cannot be exercised against the product.

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/46018>