graphax

# WARNUNG - Sofortige Sperrung aller Upload-Schnittstellen erforderlich (Apache Tomcat CVE-2025-48988/49125)

Spreitenbach, 25. Juni 2025

## Sicherheitswarnung

Im Juni 2025 wurden mehrere schwerwiegende Sicherheitslücken in Apache Tomcat entdeckt, einer zentralen Softwarekomponente, die in YSoft SafeQ 6 eingesetzt wird. Apache Tomcat dient als Webserver und verarbeitet unter anderem Datei-Uploads und verschiedene Schnittstellenanfragen. Die jetzt bekannt gewordenen Schwachstellen ermöglichen es Angreifern, gezielt Systemressourcen zu überlasten («Denial-of-Service»), Schutzmechanismen zu umgehen oder – unter bestimmten Bedingungen – unbefugt auf sensible Inhalte zuzugreifen.

---

## Betroffene Schwachstellen

**CVE-2025-48988: Denial-of-Service durch Multipart-Upload (CVSS 7.5)**
- Risiko: Systemausfall durch Ressourcenerschöpfung
- Ursache: Fehlerhafte Durchsetzung von Teilzählungsschwellenwerten

**CVE-2025-49125: Umgehung von Sicherheitskontrollen (CVSS 7.5)**
- Risiko: Unbefugter Zugriff auf geschützte Ressourcen
- Ursache: Sicherheitsbeschränkungen bei PreResources/PostResources

## Zu sperrende Schnittstellen

**End-User-Oberflächen**
- POST-Anfragen blockieren: /upload-job

**Management-Services (alle POST-Anfragen blockieren)**
- /scan/upload/*
- /software-package/packages*
- /configuration/upload-image
- /configuration/import
- /servlet/box.DashboardUploadImageServlet
- /servlet/users.ImportUsersServlet
- /servlet/web.BillingCodesCSVImportServlet
- /license/activation/upload
- /mobile-connect/credentails/import

**Payment-System (alle POST-Anfragen blockieren)**
- /manage/vouchers/import
- /manage/vouchers/vouchers-to-template
- /manage/customers/import
- /manage/quotas/*

**Information Management System**
- Alle POST-Anfragen blockieren

## Zusätzliche Sicherheitsinformationen

Entwarnung für CVE-2025-46701: Das CGI-Servlet ist in YSoft SafeQ 6 standardmässig deaktiviert - keine Massnahmen erforderlich.

## Betroffene Funktionen nach Sperrung

**Wichtiger Hinweis: Die Sperrung dieser Schnittstellen deaktiviert vorübergehend:**
- Alle Datei-Upload-Funktionen
- Import-/Export-Features
- Konfigurationsänderungen über Web-Interface
- Scan-Upload-Funktionen
- Benutzerdatenimport
- Gutschein-/Kundenimport

**Sofortige Massnahmen**
1. Firewall/Proxy konfigurieren: Blockierung aller oben genannten POST-Pfade
2. Alternative Lösung: Content-Disposition-Header-Limits einrichten (nach Absprache mit Firewall-Anbieter)
3. Zugangskontrollen: Nur autorisiertes Personal hat Tomcat-Zugriff

**Zeitplan**
- Sofort: Schnittstellen-Sperrung implementieren
- Q3 2025: Update durch Ysoft & Konica Minolta