



VIVOTEK Product Security Advisory

Advisory ID: VVTK-SA-2026-06

CVE ID: CVE-2026-65182, CVE-2026-68569, CVE-2026-101296, CVE-2026-101356, CVE-2026-103119, CVE-2026-93446, CVE-2026-88041, CVE-2026-80353

First Published: October 29th , 2026

Last Update: October 30th , 2026

Status: Confirmed

Revision: 1.0

Executive Summary

Multiple security advisories have been publicly disclosed regarding vulnerabilities in the Apache Tomcat servlet container and web server ecosystem beginning in August 2026. These disclosures address potential security constraint bypasses, HTTP/2 parser handling, and authentication bypass risks.

Following a comprehensive security architecture review, VIVOTEK confirms that no VIVOTEK product lines, device firmwares, or video management platforms utilize Apache Tomcat or Java application runtimes. Consequently, all VIVOTEK products are completely unaffected by any Apache Tomcat-related CVEs released from August 2026 onward.

Security Evaluation Conclusion: No attack surface exists within VIVOTEK solutions for Apache Tomcat exploits. Customers and system administrators do not need to apply software patches, firmware changes, or configuration workarounds.

Overview:

Target Component	Apache Tomcat / Java Servlet Container
------------------	--

Ecosystem Architecture	VIVOTEK firmware and software solutions are engineered natively using C/C++, Go, and standard platform system services with hardened embedded web servers.
Java / Tomcat Dependency	None (Zero runtime or library dependency on Java / Tomcat across all product lines)
Attack Surface	Not Present (Vulnerabilities cannot be executed or triggered on VIVOTEK products)
Customer Action Required	None

Affected Products:

The table below details the security assessment across all major VIVOTEK product lines and software architectures:

Product Family / Solution	Runtime Architecture	Status Against Tomcat CVEs
VIVOTEK IP Network Cameras & Edge AI Devices	Proprietary Embedded Linux OS (Native C/C++ daemons)	NOT AFFECTED
Standalone NVR Appliances (ND-series, RX-series)	Embedded Linux OS (Native video recording pipeline)	NOT AFFECTED
Windows-based NVR Appliances (NR Series)	Windows IoT Enterprise (No Tomcat/Java dependencies)	NOT AFFECTED
VAST Security Station (VSS) / VAST 2 VMS Host & Clients	Native Windows Client/Server Services (No Apache Tomcat components)	NOT AFFECTED
VORTEX Cloud & VSaaS Platform	Cloud Microservices / Native Services (No Apache Tomcat instances)	NOT AFFECTED

Workaround:

N/A

Because VIVOTEK solutions do not embed or run Apache Tomcat, no action, configuration change, or emergency patching is required by end users, partners, or system integrators.

Solution:

As part of ongoing cybersecurity hygiene, VIVOTEK recommends adhering to standard operational hardening practices:

- Network Segmentation: Maintain IP cameras, NVRs, and surveillance management servers on isolated VLANs segregated from general corporate and guest networks.
- Port Exposure Control: Restrict administrative web console and streaming ports to authorized administrative subnets and secure VPN connections.
- Routine Maintenance: Continue applying scheduled VIVOTEK official firmware and VMS updates to ensure cumulative security protections remain up to date.
- Credential Hygiene: Avoid default passwords and enforce robust authentication and role-based access control (RBAC) across all surveillance endpoints.

Revision History:

Revision	Date	Description
1.0	October 30, 2026	Initial release