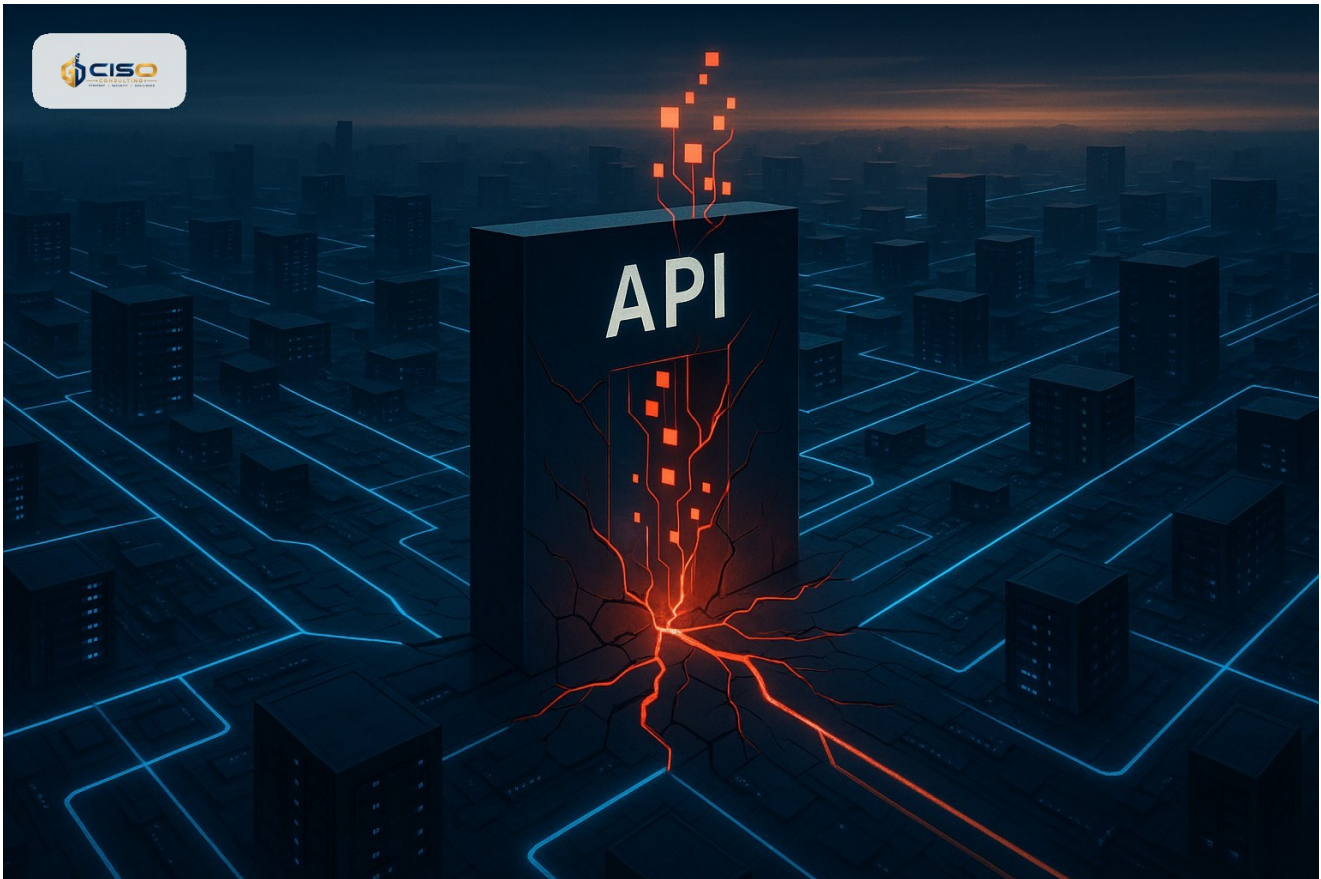


WSO2 API Products Path Traversal Vulnerability Enables Remote Code Execution



A path traversal vulnerability in WSO2 API Control Plane, API Manager, Traffic Manager and Universal Gateway permits unrestricted file upload and may lead to remote code execution.

- CVE-2026-5430 affects WSO2 API Control Plane, API Manager, Traffic Manager and Universal Gateway
- Path traversal flaw permits unrestricted file upload leading to potential remote code execution
- Organisations must apply vendor mitigations or discontinue product use if patches unavailable
- Internet-exposed assets require immediate evaluation and remediation priority

Vulnerability Overview

WSO2 has disclosed a **path traversal vulnerability** tracked as CVE-2026-5430 affecting multiple API management products. The flaw impacts WSO2 API Control Plane, API Manager, Traffic Manager and Universal Gateway. The vulnerability permits attackers to upload files without restriction, creating a pathway to remote code execution on affected systems.

Path traversal vulnerabilities allow malicious actors to access directories and files stored outside the intended folder structure. In this instance, the weakness enables unrestricted file upload capabilities that can be exploited to place executable code on vulnerable servers, granting attackers control over affected infrastructure.

Risk to Regulated Institutions

Organisations operating WSO2 API management platforms face immediate risk if systems remain unpatched. API management infrastructure typically handles authentication, authorisation and data routing for critical business services, making compromise particularly consequential for regulated entities. Successful exploitation could result in unauthorised access to sensitive data, service disruption or lateral movement within enterprise networks.

Institutions must evaluate their asset inventory to identify all deployments of affected WSO2 products, with particular attention to internet-facing instances. Cloud-hosted implementations require coordination with service providers to ensure appropriate mitigations are applied.

Remediation Guidance

Vendor mitigations should be applied immediately in accordance with WSO2 security advisories. Where patches or mitigations are unavailable, organisations must assess whether continued operation of affected products is acceptable given the risk profile, or whether temporary service discontinuation is warranted until vendor guidance becomes available. All remediation activities should be documented to demonstrate compliance with applicable cybersecurity frameworks and regulatory expectations.

What to do now

1. Conduct immediate inventory scan to identify all WSO2 API Control Plane, API Manager, Traffic Manager and Universal Gateway deployments across your environment
2. Prioritise internet-exposed WSO2 instances for immediate assessment and remediation
3. Review WSO2 vendor security advisories and apply recommended mitigations or patches without delay
4. For cloud-hosted WSO2 services, contact your service provider to confirm mitigation status and timelines
5. If vendor mitigations are unavailable, perform risk assessment to determine whether temporary service discontinuation is warranted

6. Document all remediation activities and maintain evidence for compliance reporting to NCA, SAMA or other applicable regulators