

Apache Struts Command Injection Vulnerability Requires Immediate Patching



Apache Struts contains a command injection vulnerability enabling remote attackers to execute arbitrary code when Dynamic Method Invocation is enabled, requiring immediate vendor patches.

- Apache Struts vulnerable to remote command injection via method:prefix when Dynamic Method Invocation is enabled
- Attackers can execute arbitrary code remotely without authentication
- Vendor patches and mitigations must be applied immediately
- Organizations must evaluate internet exposure of affected assets
- Discontinue product use if mitigations are unavailable

Vulnerability Overview

Apache Struts contains a **command injection vulnerability** tracked as CVE-2016-3081 that permits remote attackers to execute arbitrary code on affected systems. The vulnerability is exploitable through the method:prefix mechanism when **Dynamic Method Invocation** is enabled in the application configuration. This flaw allows unauthenticated attackers to inject and execute malicious commands remotely, presenting a significant risk to web applications built on vulnerable Struts versions.

Risk to Regulated Institutions

Organizations operating Apache Struts-based applications face immediate exposure to remote code execution attacks. The vulnerability requires no authentication, making it particularly dangerous for internet-facing applications common in banking, healthcare, and government sectors. Successful exploitation could lead to complete system compromise, data breaches, and regulatory non-compliance.

Required Response

Institutions must apply vendor-supplied patches and mitigations without delay. Organizations should conduct an inventory of all Apache Struts deployments, assess their internet exposure, and prioritize patching based on risk. Where mitigations are unavailable, affected applications should be taken offline or isolated from network access. Cloud-hosted Struts applications require coordination with service providers to ensure patches are applied. Organizations unable to patch immediately must implement compensating controls and monitor affected systems for signs of exploitation.

What to do now

1. Conduct immediate inventory of all Apache Struts deployments across your environment
2. Apply vendor-supplied patches and security updates to all affected Struts installations
3. Disable Dynamic Method Invocation in Struts configuration files where not operationally required
4. Assess internet exposure of all Struts-based applications and prioritize patching accordingly
5. Implement network segmentation and access controls to limit exposure of vulnerable systems
6. Monitor application logs and network traffic for indicators of exploitation attempts
7. Coordinate with cloud service providers to ensure patches are applied to hosted Struts applications
8. Discontinue use of affected applications or take them offline if patches cannot be applied immediately