

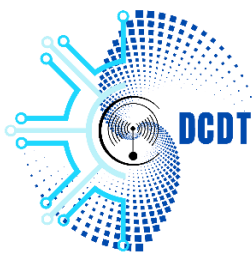
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS
& DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380



**GOVERNEMENT DE LA
REPUBLIQUE DU VANUATU**

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE
COMMUNICATION ET DE
TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu

Tel: (678) 33380

9 October 2026

Advisory 351: Apache Struts 2 Dynamic Method Invocation Remote Code Execution Vulnerability (S2-032) - Actively Exploited (CVE-2016-3081).

Release Date: 8th October 2026

Impact: **CRITICAL**

TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above product(s). This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2016-3081 (Apache Struts security bulletin S2-032) is a remote code execution vulnerability (CWE-77, command injection) in the Apache Struts 2 web application framework. When Dynamic Method Invocation is enabled, an unauthenticated remote attacker can send a request using the method: prefix to run arbitrary code on the application server. Public exploits have existed since 2016, including Metasploit modules and Exploit-DB entry 39756.

What are the systems affected?

The following Apache Struts 2 versions are affected where Dynamic Method Invocation is enabled:

- Struts 2.3.20 through 2.3.28, except 2.3.20.3 and 2.3.24.3
- NVD also lists many earlier Struts 2.0.x to 2.3.x releases, which are end of life and should be treated as vulnerable

Not affected / patched version:

- Struts 2.3.20.3, 2.3.24.3 or 2.3.28.1. Because these are very old branches, upgrade to the current supported Struts 6 or 7 release rather than staying on a patched 2.3 build

What does this mean?

Successful exploitation may allow attackers to:

- Run arbitrary commands on the application server with the privileges of the web application, without credentials
- Steal data and credentials held by the application, install web shells or malware, and use the server as a foothold into the internal network
- Be hit by automated mass scanning, since exploits are public and widely used

Mitigation process

CERTVU recommends the following:

1. Upgrade Struts

Move to a current supported Struts release. As a minimum, apply 2.3.20.3, 2.3.24.3 or 2.3.28.1, and update any commercial product that bundles Struts using the vendor's own patches.

2. Disable Dynamic Method Invocation

3. Find every Struts application

4. Add network protection

5. Hunt for compromise

Search web logs for requests with the method: parameter, and check application servers for unexpected processes, files and outbound connections. Report suspected compromise to CERTVU.

Reference

1. <https://cwiki.apache.org/confluence/display/WW/S2-032>
2. <https://nvd.nist.gov/vuln/detail/CVE-2016-3081>
3. <https://app.opencve.io/cve/CVE-2016-3081>
4. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>