

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Apache Struts Flaw Exploited for Remote Code Execution in Active Attacks

Date of Publication

December 18, 2024

Admiralty Code

A1

TA Number

TA2024464




Summary

First Seen: December 2024

Affected Products: Apache Struts 2 and 6 versions

Impact: Apache has released a patch for a critical vulnerability in Struts, identified as CVE-2024-53677. This flaw allows remote attackers to execute arbitrary code, posing significant risks of critical data loss and full system compromise. Alarming, CVE-2024-53677 is being actively exploited in the wild, with attackers leveraging public proof-of-concept exploits to identify and target vulnerable systems.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-53677	Apache Struts Remote Code Execution Vulnerability	Apache Struts 2 and 6 versions			

Vulnerability Details

#1

A critical vulnerability in Apache Struts, tracked as CVE-2024-53677, has come under active exploitation, with attackers leveraging public proof-of-concept exploits to identify and target unpatched systems. Apache Struts is a widely adopted open-source framework for building Java-based web applications. Its Model-View-Controller (MVC) architecture enables developers to build enterprise-grade applications with robust features like data validation and seamless integration with other frameworks.

#2

This vulnerability resides in the file upload mechanism of Apache Struts. By manipulating file upload parameters, attackers can bypass security mechanisms to perform path traversal and upload files to arbitrary server locations. Additionally, they can achieve remote code execution (RCE) by uploading and executing malicious files, such as .jsp scripts or binary payloads. These exploits allow adversaries to compromise servers, potentially leading to data theft, unauthorized access, or full system control.

#3

The vulnerability is specific to deprecated File Upload Interceptor and patch is not backward compatible requiring implementations to urgently move to Action File Upload Interceptor. Given the widespread adoption of the framework, this flaw presents a significant threat to enterprise environments, demanding immediate action. Organizations are strongly advised to apply available patches and review their security postures to protect against ongoing exploitation.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-53677	Struts Version 2.0.0 - Struts 2.3.37 (EOL), Struts Version 2.5.0 - Struts 2.5.33, Struts Version 6.0.0 - Struts 6.3.0.2	cpe:2.3:a:apache:struts:*:*:*:*:*:*:*:*	CWE-434

Recommendations



Apply Updated Patches Immediately: Upgrade Apache Struts to the latest patched version to mitigate the vulnerability.



Review and Secure File Upload Mechanisms: Ensure proper validation and sanitization of file upload parameters to prevent path traversal or the execution of malicious files. Use secure configurations for the file upload feature.



Restrict File Upload Permissions: Limit file upload directories to specific, isolated locations and apply strict permissions to prevent execution of uploaded files.



Implement Web Application Firewalls (WAFs): Implement a WAF to filter malicious requests, including those attempting to exploit this vulnerability, and monitor for suspicious activities.

Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0001</u> Initial Access	<u>TA0002</u> Execution	<u>T1588</u> Obtain Capabilities
<u>T1588.006</u> Vulnerabilities	<u>T1190</u> Exploit Public-Facing Application	<u>T1059</u> Command and Scripting Interpreter	<u>T1059.007</u> JavaScript

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	169[.]150[.]226[.]162

Patch Details

Update to Struts 6.4.0 or a later version and transition to the updated file upload mechanism to address the vulnerability.

Link: <https://struts.apache.org/download.cgi>

References

<https://cwiki.apache.org/confluence/display/WW/S2-067>

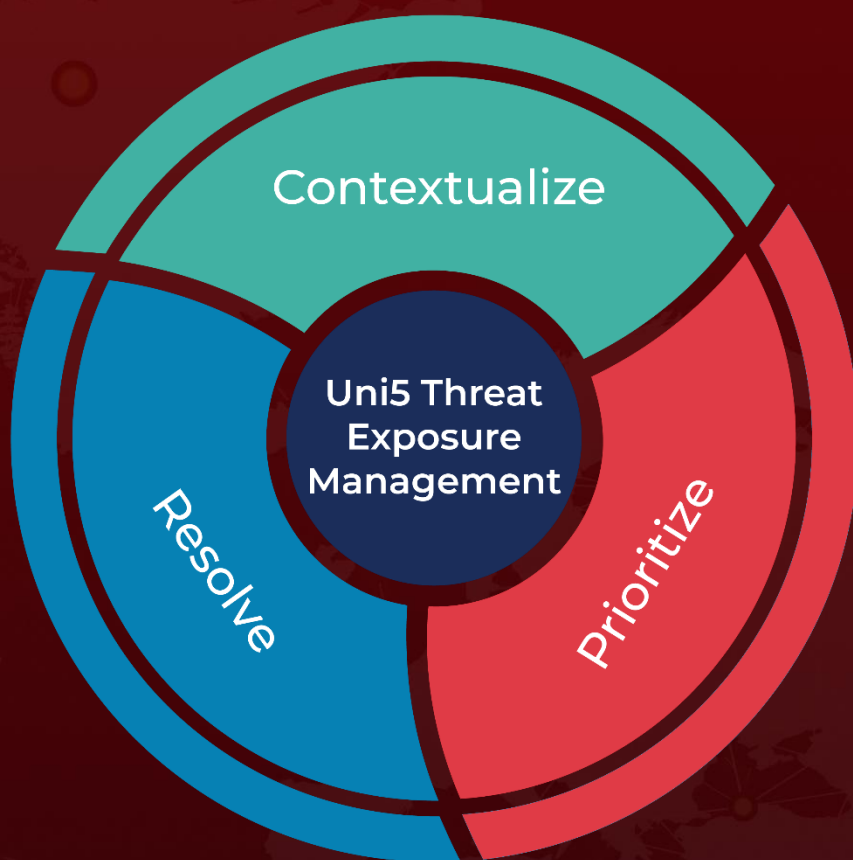
<https://github.com/TAM-K592/CVE-2024-53677-S2-067>

<https://isc.sans.edu/diary/Exploit+attempts+inspired+by+recent+Struts2+File+Upload+Vulnerability+CVE202453677+CVE202350164/31520/>

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

December 18, 2024 • 7:45 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com