

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Critical Remote Code Execution Flaw Uncovered in Apache Struts 2

Date of Publication

December 14, 2023

Admiralty Code

A1

TA Number

TA2023503




Summary

First Seen: December 7, 2023

Affected Product: Apache Struts

Impact: A significant vulnerability has been identified in the Apache Struts 2 open-source web application framework, labeled CVE-2023-50164. This flaw poses a severe risk of remote code execution and unauthorized path traversal.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-50164	Apache Struts2 Remote Code Execution Vulnerability	Apache Struts			

Vulnerability Details

#1

Apache has issued a security alerting users to a pivotal security vulnerability within the Struts 2 open-source web application framework, posing a severe risk of remote code execution. Identified as CVE-2023-50164, this vulnerability originates from a flawed "file upload logic," potentially enabling unauthorized path traversal. Under specific conditions, malevolent actors could exploit this flaw to upload a malicious file, ultimately achieving arbitrary code execution.

#2

Adversaries are actively seeking to exploit a recently remedied critical vulnerability, relying on publicly available proof-of-concept exploit code. In the event of successful exploitation, a threat actor could manipulate sensitive files, exfiltrate data, disrupt crucial services, or maneuver laterally within the network. Such actions may result in unauthorized access to web servers, compromise or theft of sensitive data, disturbance of critical services, and lateral movement within compromised networks. However, there is no substantiated evidence indicating malicious exploitation of this vulnerability in real-world attacks.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-50164	Struts 2.3.37 (EOL) Struts 2.5.0 - Struts 2.5.32, and Struts 6.0.0 - Struts 6.3.0	cpe:2.3:a:apache:struts :*:*:*:*:*:*	CWE-552

Recommendations



Apply Official Fixes Immediately: It is crucial to promptly apply the security patch provided by Apache to address the identified vulnerability (CVE-2023-50164) in the Struts 2 open-source web application framework.



Secure Configuration Management: Maintain a secure configuration baseline for all systems and applications. This involves disabling unnecessary services, configuring security settings, and adhering to industry best practices to minimize the attack surface.



Anomaly Detection: Implement anomaly detection algorithms to identify deviations from normal network behavior. This includes monitoring network traffic, system logs, and user activities for any unusual patterns.



Zero Trust Architecture: Consider adopting a Zero Trust Architecture, which assumes that threats can exist both outside and inside the network. Implement strict access controls, multi-factor authentication, and least privilege principles to limit access to sensitive resources.



Encryption and Network Segmentation: Implement strong encryption for data in transit and at rest. Additionally, network segmentation limits lateral movement within the network, isolating critical assets from potential compromise.



Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0001</u> Initial Access	<u>TA0002</u> Execution	<u>TA0003</u> Persistence
<u>TA0004</u> Privilege Escalation	<u>TA0008</u> Lateral Movement	<u>T1059</u> Command and Scripting Interpreter	<u>T1588</u> Obtain Capabilities
<u>T1574</u> Hijack Execution Flow	<u>T1040</u> Network Sniffing	<u>T1505</u> Server Software Component	<u>T1068</u> Exploitation for Privilege Escalation
<u>T1587.004</u> Exploits	<u>T1587</u> Develop Capabilities	<u>T1588.006</u> Vulnerabilities	

Patch Details

The bug has been addressed through patches, which are available in versions 2.5.33 and 6.3.0.2 or later. It is highly recommended to perform this upgrade to ensure system security.

Links:

<https://struts.apache.org/download.cgi#struts-ga>

References

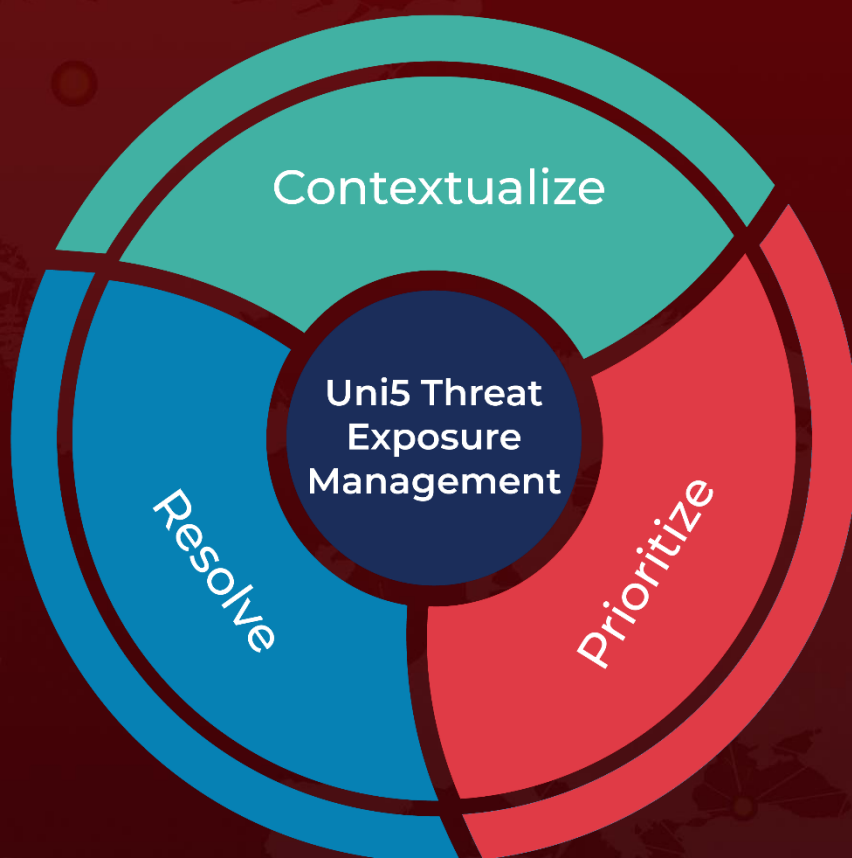
<https://lists.apache.org/thread/yh09b3fkf6vz5d6jdgrlvmg60lftqhj>

<https://struts.apache.org/announce-2023#a20231207-1>

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 14, 2023 • 4:00 AM

© 2023 All Rights are Reserved by Hive Pro®



More at www.hivepro.com