

HiveForce Labs

THREAT ADVISORY



VULNERABILITY REPORT

Zero-Day Authentication Bypass Exploit in Apache OFBiz

Date of Publication

December 29, 2023

Admiralty Code

A1

TA Number

TA2023527







Summary

First Seen: December 26, 2023

Affected Platform: Apache OFBiz

Impact: CVE-2023-51467 is a critical authentication bypass vulnerability in Apache OFBiz. Exploitation of this vulnerability could result in bypass authentication to achieve a simple Server-Side Request Forgery (SSRF) or arbitrary code execution. Users are advised to update to Apache OFBiz version 18.12.11 to mitigate potential risks.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-51467	Apache OFBiz Pre-authentication Remote Code Execution Vulnerability	Apache OFBiz			
CVE-2023-49070	Apache OFBiz Pre-authentication Remote Code Execution Vulnerability	Apache OFBiz			

Vulnerability Details

#1

A critical vulnerability has been identified as CVE-2023-51467 in Apache OFBiz, an open-source enterprise resource planning system, and is actively being exploited through publicly available proof-of-concept exploits. Researchers uncovered the CVE-2023-51467 while investigating the root cause of a previously disclosed vulnerability, CVE-2023-49070.

#2

The patch released for CVE-2023-49070, which aimed to address the issue, was found to be incomplete, leaving an authentication bypass vulnerability intact. Apache initially removed the XML RPC code from the application to fix CVE-2023-49070, but subsequent analysis revealed that the flaw persisted in the login functionality.

#3

The pre-authentication remote code execution flaw (CVE-2023-49070) allows attackers to gain elevated privileges, execute arbitrary code, and access sensitive information without authentication. This vulnerability has implications for Atlassian JIRA, a widely used commercial project management software. The issue (CVE-2023-51467) has been addressed in OFBiz version 18.12.11. Ongoing scans using public exploits underscore the urgency of upgrading to the latest release (18.12.11) to mitigate potential risks.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-51467	Apache OFBiz before 18.12.11	cpe:2.3:a:apache:ofbiz:*:*:*:*:*:*	CWE-918 CWE-287
CVE-2023-49070	Apache OFBiz before 18.12.10	cpe:2.3:a:apache:ofbiz:*:*:*:*:*:*	CWE-94

Recommendations



Apply Security Updates: Upgrade Apache OFBiz to version 18.12.11 or newer, which includes the fix for CVE-2023-51467. This step is crucial to ensure that the authentication bypass vulnerability is addressed. Regularly check for and apply security patches and updates provided by the Apache OFBiz project.



Intrusion Prevention System (IPS): Deploy and update intrusion prevention systems (IPS) that can detect and block exploit attempts related to CVE-2023-51467.



Deploy Anomaly Detection and Monitoring: Implement network monitoring tools with anomaly detection capabilities to identify unusual or suspicious patterns of network activity. This can include unexpected increases in data traffic, unusual access patterns, or deviations from normal behavior.



Network Segmentation: Implement network segmentation to restrict unauthorized access to sensitive systems. Isolate critical servers and databases from less secure parts of the network, reducing the potential impact of a successful attack.

Potential MITRE ATT&CK TTPs

<u>TA0002</u> Execution	<u>TA0042</u> Resource Development	<u>TA0001</u> Initial Access	<u>TA0004</u> Privilege Escalation
<u>T1059</u> Command and Scripting Interpreter	<u>T1203</u> Exploitation for Client Execution	<u>T1588.005</u> Exploits	<u>T1659</u> Content Injection
<u>T1588</u> Obtain Capabilities	<u>T1588.006</u> Vulnerabilities	<u>T1068</u> Exploitation for Privilege Escalation	

Patch Details

Upgrade Apache OFBiz to version 18.12.11 or newer version

Links:

<https://issues.apache.org/jira/browse/OFBIZ-12873>

<https://issues.apache.org/jira/browse/OFBIZ-12812>

<https://ofbiz.apache.org/download.html>

References

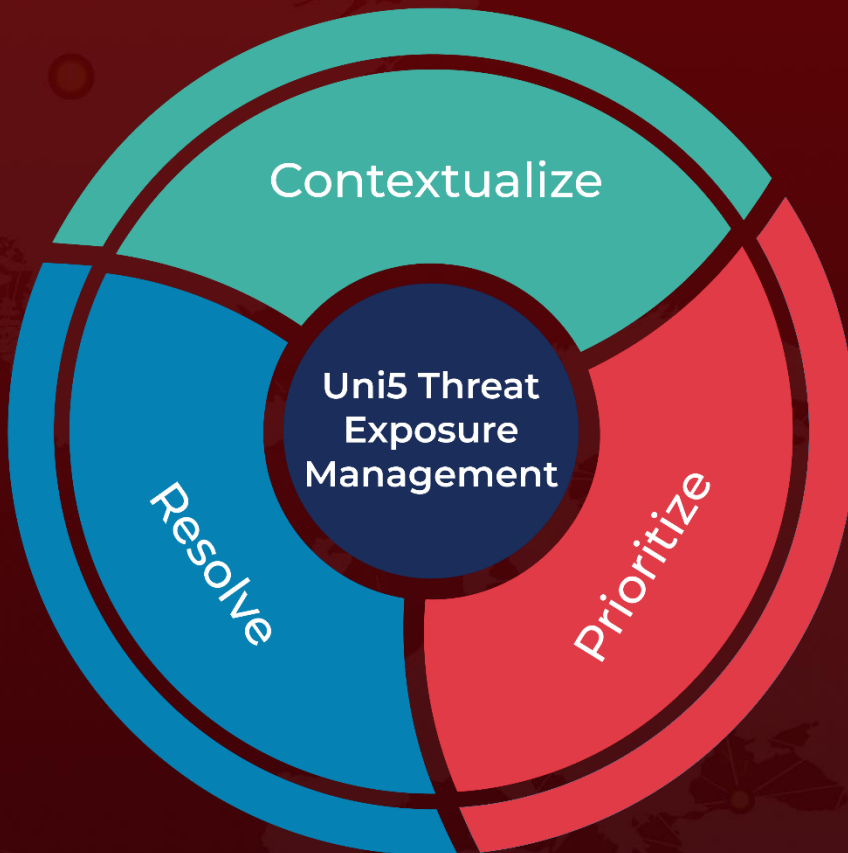
<https://blog.sonicwall.com/en-us/2023/12/sonicwall-discovers-critical-apache-ofbiz-zero-day-authbiz/>

<https://lists.apache.org/thread/9tmf9qyyhgh6m052rhz7lg9vxn390bdv>

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 29, 2023 • 5:30 AM

© 2023 All Rights are Reserved by Hive Pro[®]



More at www.hivepro.com