Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Apache OFBiz Flaw Enables Attackers to Execute Remote Code

Date of Publication	Admiralty Code	TA Number
August 6, 2024	A1	TA2024297

Summary

First Seen: August 2024
Affected Products: Apache OFBiz
Impact: A pre-authentication remote code execution vulnerability, CVE-2024-38856, has been disclosed in Apache OFBiz. This vulnerability could allow threat actors to achieve remote code execution on affected instances, posing a significant threat to organizations using this open-source enterprise resource planning (ERP) system.

⚙ CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-38856	Apache OFBiz Incorrect Authorization Vulnerability	Apache OFBiz	✗	✓	✓

Vulnerability Details

#1 Apache OFBiz, an open-source ERP system renowned for its extensive customization and support for various industries, automates and integrates diverse business processes, including accounting, human resources, customer relationship management, order management, manufacturing, and e-commerce. Recently, researchers uncovered a critical pre-authentication remote code execution vulnerability, CVE-2024-38856, during an analysis of a previously patched issue (CVE-2024-36104).

#2 This vulnerability, rated with a CVSS score of 9.8, stems from a flaw in the override view functionality, which inadvertently exposes essential endpoints to unauthenticated attackers. By manipulating specific request parameters, adversaries can circumvent authentication checks and access restricted endpoints, thereby facilitating remote code execution and posing a significant threat to organizations using the affected ERP system.

#3 The core issue lies in the inconsistency between the two URI calculation methods, which can be exploited to bypass authentication and security checks. When the server receives a request, it initializes the variables path, requestUri, and overrideViewUri. The methods getRequestUri and getOverrideViewUri are tasked with calculating these variables. However, a discrepancy arises in the return values for the path.

#4 This discrepancy creates a flaw in the authentication mechanism, as authz checks are conducted on `requestUri`, but the page associated with `overrideViewUri` is rendered instead. This mismatch leads to confusion within the authentication process, allowing threat actors to bypass the patch for CVE-2024-36104 and execute code.

#5 The vulnerability opens the door for unauthenticated remote code execution. Although there is no evidence of the vulnerability being exploited as a zero-day, the availability of a proof of concept (PoC) within a day raises concerns about possible exploitation.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-38856	Apache OFBiz versions up to 18.12.14	cpe:2.3:a:apache:ofbiz:18.12.14:*:*:*:*:*:*:*	CWE-863

Recommendations

Update: To mitigate the risk associated with CVE-2024-38856, users are strongly urged to upgrade their Apache OFBiz installations to version 18.12.15. This update addresses the pre-authentication remote code execution vulnerability and enhances the overall security of the ERP system.

Deploy Behavioral Analysis Solutions: Utilize behavioral analysis solutions to detect any anomalous behavior on systems. Ensure that endpoint protection solutions are regularly updated to identify and mitigate the latest threats.

Least Privilege: Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks, restrict the access to the trusted parties only. This strategy reduces the effects of vulnerabilities related to privilege escalation.

Limit Exposure: Restrict access to critical systems and endpoints to minimize potential attack vectors. Implement strict network access controls to ensure that only authorized users and systems can interact with sensitive components.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities	**T1190** Exploit Public-Facing Application
T1059 Command and Scripting Interpreter	**T1556** Modify Authentication Process	**T1068** Exploitation for Privilege Escalation	

Patch Details

Users are strongly urged to upgrade their Apache OFBiz installations to version 18.12.15. This update addresses the CVE-2024-38856 and enhances the overall security of the ERP system.

Link: https://ofbiz.apache.org/download.html

References

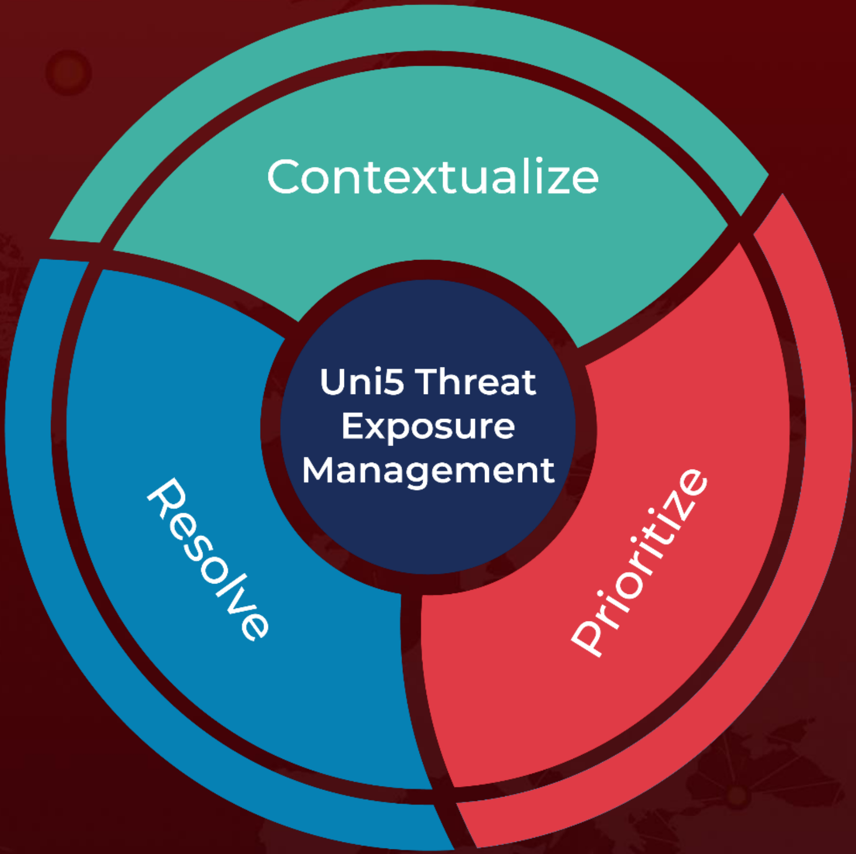
https://blog.sonicwall.com/en-us/2024/08/sonicwall-discovers-second-critical-apache-ofbiz-zero-day-vulnerability/

https://lists.apache.org/thread/olxxjk6b13sl3wh9cmp0k2dscvp24l7w

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

August 6, 2024 • 6:50 AM

More at www.hivepro.com