Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Apache Addresses Persistent RCE Flaw in OFBiz

Date of Publication	Admiralty Code	TA Number
September 6, 2024	A1	TA2024342

Summary

First Seen: August 2024
Affected Products: OFBiz (Open For Business) software
Impact: Apache has addressed a critical security vulnerability in its open-source OFBiz software, identified as CVE-2024-45195. This remote code execution (RCE) flaw stems from a forced browsing weakness, which allows attackers to bypass access controls and gain access to restricted paths. By exploiting this vulnerability, an unauthenticated attacker could send specially crafted requests, leading to the execution of arbitrary code on the affected system.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-45195	Apache OFBiz Unauthenticated Remote Code Execution Vulnerability	Apache OFBiz	✗	✗	✓

Vulnerability Details

#1 Apache OFBiz has discovered an unauthenticated remote code execution falw on both Linux and Windows platforms. This critical vulnerability, identified as CVE-2024-45195, is rooted in a forced browsing weakness that exposes restricted paths to unauthenticated direct requests. Attackers can exploit missing view authorization checks within the web application, allowing them to execute arbitrary code on the server without needing valid credentials.

#2 The application's approach to parsing the request URI is causing fragmentation in the controller and view map. This fragmentation is due to the use of multiple different methods for parsing the request URI, with one method used to determine the controller and another used to map the view.

#3 This architectural flaw enables attackers to exploit the system by accessing and interacting with authenticated view maps through unauthenticated controllers. The fragmentation between the application's controller and view map has led to several vulnerabilities, including CVE-2024-32113, CVE-2024-36104, and CVE-2024-38856. While patches have been released for these CVEs, they only address specific exploitation techniques and do not resolve the underlying architectural issue.

#4 The Apache security team has finally patched the flaw in version 18.12.16 of OFBiz by implementing stronger authorization checks. Users are strongly advised to upgrade their installations immediately to protect their systems from these recurring vulnerabilities and prevent potential exploitation.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-45195	Apache OFBiz: Version Prior to 18.12.16	cpe:2.3:a:apache:ofbiz:*:*:*:*:*:*:*:*	CWE-425

Recommendations

Update: Apache has patched the critical vulnerability CVE-2024-45195 in version 18.12.16 of OFBiz by implementing authorization checks. OFBiz users are strongly advised to upgrade their installations to this latest version as soon as possible to safeguard their systems against potential attacks.

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.

Implement Web Application Firewall (WAF): Deploy a WAF to monitor and filter incoming web traffic. A properly configured WAF can detect and block attempts to exploit the vulnerabilities, providing an additional layer of protection.

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.

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	T1068 Exploitation for Privilege Escalation	T1556 Modify Authentication Process	

Patch Details

Users are strongly encouraged to update to the latest version, Apache OFBiz 18.12.16, to prevent unauthorized access and reduce the risk of potential remote code execution (RCE).

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

References

https://www.rapid7.com/blog/post/2024/09/05/cve-2024-45195-apache-ofbiz-unauthenticated-remote-code-execution-fixed/

https://ofbiz.apache.org/security.html

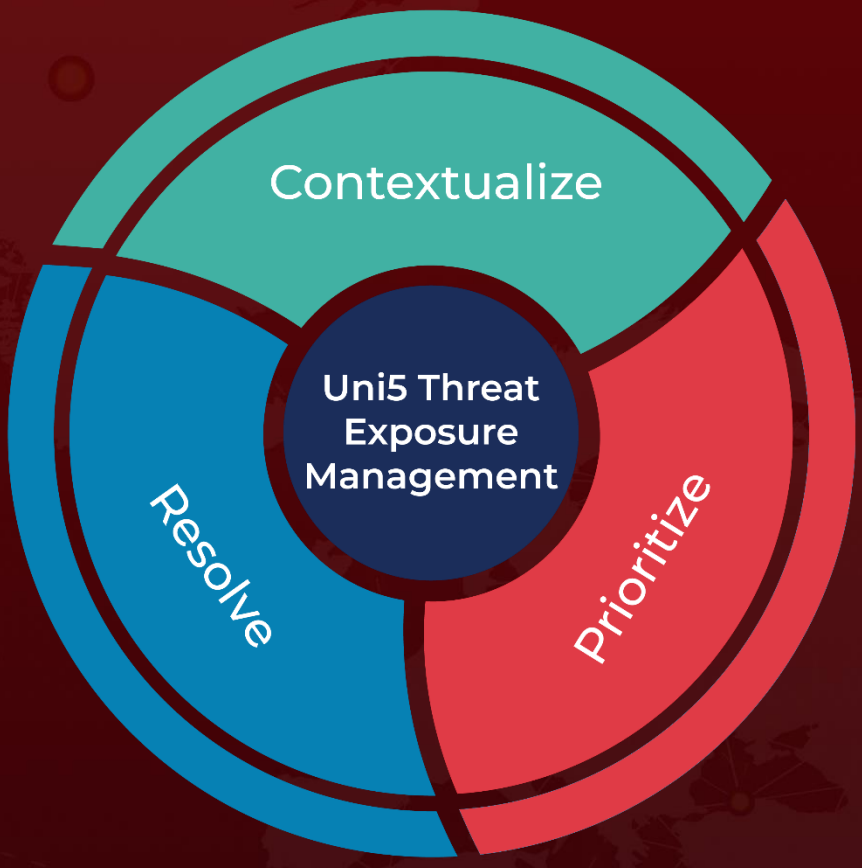
https://hivepro.com/threat-advisory/apache-ofbiz-flaw-enables-attackers-to-execute-remote-code/

https://hivepro.com/threat-digest/cisa-known-exploited-vulnerability-catalog-august-2024/

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

September 6, 2024 . 7:00 AM

More at www.hivepro.com