

Apache OFBiz RCE Attack

Actively Targeted Zero-day

<https://ofbiz.apache.org/security.html>
 CVEs: [CVE-2024-38856](#), [CVE-2024-36104](#)

FortiGuard Labs continues to observe attack attempts targeting the recent Apache OFBiz vulnerabilities (CVE-2024-38856 and CVE-2024-36104) that can be exploited by threat actors through maliciously crafted unauthorized requests, leading to the remote code execution.

Background Apache OFBiz is an open-source enterprise resource planning (ERP) system that provides business solutions to various industries. It includes tools to manage business operations such as customer relationships, order processing, human resource functions, and more. According to open sources, there are hundreds of companies worldwide that use Apache OFBiz.

CVE-2024-38856 is an Incorrect Authorization vulnerability, meaning that an unauthenticated user can access restricted functionalities. This flaw was identified while analyzing the patch for CVE-2024-36104, which was an incomplete fix.

CVE-2024-36104 is a Path Traversal vulnerability in Apache OFBiz that exposes endpoints to unauthenticated users, who could leverage it to achieve remote code execution via specially crafted requests.

Latest Developments FortiGuard Labs recommends users of the Apache OFBiz application to upgrade to version 18.12.15 or later to mitigate the security vulnerabilities (CVE-2024-38856 and CVE-2024-36104).

August 27, 2024: CISA added Apache OFBiz Incorrect Authorization Vulnerability (CVE-2024-38856) to its known exploited vulnerabilities catalog (KEV).
<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

August 5, 2024: Researchers at Sonicwall discovers Apache OFBiz Zero-Day Vulnerability (CVE-2024-38856).
<https://blog.sonicwall.com/en-us/2024/08/sonicwall-discovers-second-critical-apache-ofbiz-zero-day-vulnerability/>

June 3, 2024: CVE-2024-36104 was disclosed by OSS-Security.
<https://www.openwall.com/lists/oss-security/2024/06/03/1>






PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

- Reconnaissance
- Weaponization
- Delivery
- Exploitation


IPS

Detects and blocks attack attempts leveraging the vulnerability

 FortiADC DB 28.847	 FortiGate DB 28.847	 FortiNDR DB 28.847	 FortiProxy DB 28.847	 FortiSASE DB 28.847
--	---	--	--	---

Web App Security

Detects and blocks attack attempts leveraging the vulnerability

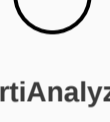
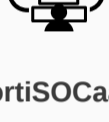

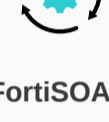
 FortiWeb

- Installation
- C2
- Action

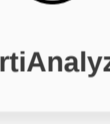
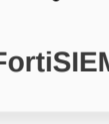
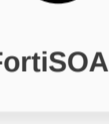
DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

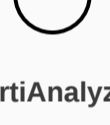
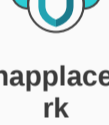
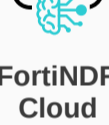

IOC

 FortiAnalyzer	 FortiSOCaaS	 FortiSIEM	 FortiSOAR
--	--	--	--

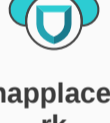
Outbreak Detection

 FortiAnalyzer DB 2.00052	 FortiSIEM DB 612	 FortiSOAR v7.4
--	--	--

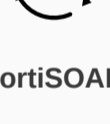
Threat Hunting

 FortiAnalyzer	 Fcnapplacework	 FortiNDR Cloud	 FortiSIEM
--	---	---	--

Cloud Threat Detection

 Fcnapplacework

Playbook

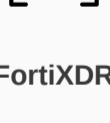
 FortiSOAR v7.4
--

RESPOND

Develop containment techniques to mitigate impacts of security events:

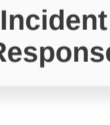
Automated Response

Services that can automatically respond to this outbreak.

 FortiXDR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.



 Incident Response
--

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.

 NSE Training	 Response Readiness
---	---

End-User Training

Raise security awareness to your employees that are continuously being targeted by phishing, drive-by download and other forms of cyberattacks.



 Security Awareness & Training
--

IDENTIFY

Identify processes and assets that need protection:

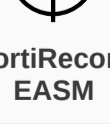
Attack Surface Hardening

Check Security Fabric devices to build actionable configuration recommendations and key indicators.

 Security Rating	 FortiDAST
--	--

Attack Surface Monitoring (Inside & Outside)

Security reconnaissance and penetration testing services, covering both internal & external attack vectors, including those introduced internally via software supply chain.

 FortiRecon: EASM

Additional Resources

CVE-2024-38856 <https://lists.apache.org/thread/olxxjk6b13sl3wh9cm0k2dscvp24l7w>

CVE-2024-36104 <https://issues.apache.org/jira/browse/OFBIZ-13092>

About Apache OFBiz <https://enllyft.com/tech/products/apache-ofbiz>

Learn more about [FortiGuard Outbreak Alerts](#)