FORTINET

FortiGuard Labs Outbreak Alerts

Apache OFBiz RCE Attack

Actively Targeted Zero-day

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

CVEs: CVE-2024-32113,CVE-2024-38856,CVE-2024-36104,CVE-2024-45195

FortiGuard Labs continues to observe attack attempts targeting the recent Apache OFBiz vulnerabilities (CVE-2024-38856, CVE-2024-45195 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.

CVE-2024-45195 is a Direct Request ('Forced Browsing') vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 18.12.16. Users are recommended to upgrade to version 18.12.16, which fixes the issue.

Latest Developments

FortiGuard Labs recommends users of the Apache OFBiz application to upgrade to version 18.12.16 or later to mitigate the security vulnerabilities including the latest (CVE-2024-45195).

- February 04, 2025: CISA added Apache OFBiz Forced Browsing Vulnerability (CVE-2024-45195) to its known exploited vulnerabiltites (KEV) catalog.
- September 04, 2024: Apache OFBiz advisory published for CVE-2024-45195, which has surfaced by bypassing previous patches for CVE-2024-32113, CVE-2024-36104, and CVE-2024-38856.
  https://issues.apache.org/jira/browse/OFBIZ-13130
- August 27, 2024: CISA added Apache OFBiz Incorrect Authorization Vulnerability (CVE-2024-38856) to its known exploited vulnerabilitites catalog (KEV).
  https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- August 05, 2024: Researchers at Sonicwal 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 03, 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:

IPS

Detects and blocks attack attempts leveraging the vulnerability

FortiADC — DB 30.953
FortiGate — DB 30.953
FortiNDR — DB 30.953
FortiProxy — DB 30.953
FortiSASE — DB 30.953

Web App Security

Detects and blocks attack attempts leveraging the vulnerability

FortiWeb

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
Lacework CNAPP
FortiNDR Cloud
FortiSIEM

Cloud Threat Detection

Lacework CNAPP

Playbook

FortiSOAR — v7.4

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automaticlly 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 (Apache)	https://lists.apache.org/thread/olxxjk6b13sl3wh9cmp0k2dscvp24l7w
CVE-2024-36104 (Apache)	https://issues.apache.org/jira/browse/OFBIZ-13092
About Apache OFBiz	https://enlyft.com/tech/products/apache-ofbiz
CVE-2024-45195 (Apache)	https://issues.apache.org/jira/browse/OFBIZ-13130

Learn more about FortiGuard Outbreak Alerts