

CVE-2024-38856

Apache OFBiz Incorrect Authorization Vulnerability

Exigent

CISA KEV since Aug 27, 2024

Actively exploited

Public exploit module (Metasploit)

Incorrect Authorization vulnerability in Apache OFBiz. This issue affects Apache OFBiz: through 18.12.14. Users are recommended to upgrade to version 18.12.15, which fixes the issue. Unauthenticated endpoints could allow execution of screen rendering code of screens if some preconditions are met (such as when the screen definitions don't explicitly check user's permissions because they rely on the configuration of their endpoints).

EVRS 87 / 100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.994 99.94th percentile · FIRST	CISA DEADLINE Sep 17, 2024 KEV since 2024 · listed over a year
--	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.994 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable. **CISA note:** This vulnerability affects a common open-source component, third-party library, or a protocol used by different products. Please check with specific vendors for information on patching status.
Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
ofbiz	< 18.12.15	18.12.15	NVD

Sources

Vendor guidance	ofbiz.apache.org/security.html	Additional guidance	lists.apache.org/thread/olxxjk6b13sl3wh9cmp0k2dscvp24l7w
NVD	nvd.nist.gov/vuln/detail/CVE-2024-38856	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2024-37643	Current data	evulnable.com/vulnerability-management/cve/CVE-2024-38856

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.