CERT-EU

Security Advisory 2024-003

Critical Vulnerability in Apache OFBiz

January 9, 2024 — v1.0

TLP:CLEAR

History:

- *09/01/2024 — v1.0 – Initial publication*

Summary

On December 26, 2023, the Apache OFBiz project released an update addressing a critical vulnerability in Apache OFBiz. The vulnerability allows attackers to bypass authentication, which could lead to remote code execution (RCE) [1].

Technical Details

The vulnerability, identified as **CVE-2023-51467** with a CVSS score of 9.8 [2], may allow an attacker to bypass authentication to achieve a simple Server-Side Request Forgery (SSRF). A successful exploit may allow the attacker to perform remote code execution.

Affected Products

This vulnerability affects Apache OFBiz versions below 18.12.11 [3,4].

Recommendations

It is recommended to upgrade to version 18.21.11 as soon as possible.

References

[1] https://lists.apache.org/thread/9tmf9qyyhgh6m052rhz7lg9vxn390bdv

[2] https://nvd.nist.gov/vuln/detail/CVE-2023-51467

[3] https://issues.apache.org/jira/browse/OFBIZ-12873

[4] https://ofbiz.apache.org/release-notes-18.12.11.html