Computer Emergency Response Team of Mauritius
Ministry of Information Technology, Communication and Innovation

CERT-MU Vulnerability Note

Apache Jackrabbit Vulnerability Exposes Systems to Remote Code Execution Attacks

Vulnerability Note: VN-2025-24

Date of Issue: 08 September 2025

Severity Rating: High

Systems Affected:

- Apache Jackrabbit Core, JCR Commons versions 1.0.0 through 2.22.1

Description

A new security flaw has been discovered in Apache Jackrabbit, a widely used content repository system, potentially exposing thousands of applications to remote code execution (RCE) risks. The issue arises from deserialization of untrusted data within JNDI-based repository lookups. Attackers can exploit this by injecting malicious JNDI references when applications accept untrusted inputs for repository connections. Once triggered, the flaw may allow attackers to execute arbitrary code on the target system, compromising sensitive data and system stability.

CVE Information
CVE-2025-58782

Workaround
Users are advised to upgrade to Jackrabbit 2.22.2 without delay. For those unable to upgrade immediately, disabling JNDI lookups for JCR connections is advised.
More information is available on:
https://seclists.org/oss-sec/2025/q3/151

Postal address
Mauritian Computer Emergency Response Team (CERT-MU)
Ministry of Information Technology, Communication and Innovation
2nd Floor, Wing A,
Shri Atal Bihari Vajpayee Tower,
Cybercity Ebene