مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Apache CloudStack

Tracking #:432318934

Date:11-05-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Apache CloudStack has released security updates addressing multiple vulnerabilities affecting CloudStack deployments, including an important unauthenticated command injection flaw that could enable arbitrary code execution on KVM hosts, along with multiple access control, privilege escalation, and denial-of-service issues.

TECHNICAL DETAILS:

Vulnerability Details
Important Severity

- **CVE-2026-25077**
  - An unauthenticated command injection vulnerability in Direct Download Templates allows attackers to exploit insufficient filename sanitization to execute arbitrary code on KVM hosts. Successful exploitation can result in full infrastructure compromise, data loss, denial of service, and host-level control.
- **CVE-2025-66171**
  - Improper access control in the Backup plugin allows authenticated users to create virtual machines from backups belonging to other users, leading to unauthorized access to sensitive backup data and resources.
- **CVE-2025-66172**
  - Improper authorization in the Backup plugin enables authenticated users to restore volume backups from other tenants and attach them to their own virtual machines, resulting in cross-tenant data access.
- **CVE-2025-66467**
  - Missing cleanup of MinIO policies during bucket deletion allows previous bucket owners to retain access permissions. If a bucket name is reused, attackers may gain unauthorized read/write access using previously issued credentials.

Moderate Severity

- **CVE-2025-69233**
  - Race conditions and missing validations in resource quota enforcement allow users to exceed allocated domain or account limits, potentially leading to resource exhaustion and denial-of-service conditions.
- **CVE-2026-25199**
  - The Proxmox extension incorrectly trusts a user-editable VM identifier (proxmox_vmid), enabling attackers to modify it and gain unauthorized cross-tenant access and full control over other users' virtual machines.

Low Severity Vulnerabilities

- **CVE-2025-66170**
  - Improper authorization in the Backup plugin allows authenticated users to list backup metadata belonging to other accounts, exposing unauthorized backup visibility.

Affected Versions

- Apache CloudStack 4.0.0 through 4.22.0.0

Fixed Versions

- Apache CloudStack LTS 4.20.3.0 and 4.22.0.1 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Apache CloudStack.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://lists.apache.org/thread/n8mt5b7wkpysstb8w7rr9f02kc5cq2xm