مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates – Apache Linkis

Tracking #:432316119

Date:06-08-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Apache released security updates to address multiple vulnerabilities in its product; Linkis.

TECHNICAL DETAILS:

Apache Linkis, the popular computation middleware widely used to connect applications with various data processing engines, has addressed two significant security vulnerabilities that could have exposed users to potential attacks.

Vulnerability Details:

- **CVE-2024-27181** | Privilege Escalation Attack vulnerability
  - Privilege Escalation in Basic management services where the attacking user is a trusted account allows access to Linkis's Token information.

- **CVE-2024-27182** | Engine material management Arbitrary file deletion vulnerability
  - A user with an administrator account could delete any file accessible by the Linkis system user.

Affected Versions:

- Apache Linkis versions <= 1.5.0

Fixed Versions:

- Apache Linkis version 1.6.0

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by Apache.

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/hosd73l7hxb3rpt5rb0yg0ld11zph4c6
- https://lists.apache.org/thread/2of1p433h8rbq2bx525rtftnk19oz38h