



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Multiple Vulnerabilities in Apache Products

Tracking #:432315652

Date:26-02-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Multiple Vulnerabilities in Apache Products that could be exploited to execute malicious code on vulnerable systems.

TECHNICAL DETAILS:

Vulnerabilities Details:

1.CVE-2024-23673

- CVSS Base Score: 8.5 HIGH
- A vulnerability exists in Apache Sling Servlets Resolver that could allow an attacker to execute malicious code on a vulnerable system. This vulnerability is caused by path traversal, which could allow an attacker to trick the application into loading a script from a location that it should not have access to.

2.CVE-2023-50943

- CVSS Base Score: 7.5 HIGH
- A vulnerability exists in Apache Airflow that allows an attacker to tamper with XCom data through a deserialization vulnerability. An attacker can exploit this vulnerability to potentially inject arbitrary code into the system, leading to unauthorized access or complete system takeover.

Affected Versions:

Apache Sling Servlets Resolver v2.10.0

Apache Airflow v2.8.0

Fixed Versions:

Apache Sling Servlets Resolver v2.11.0

Apache Airflow v2.8.1 or later

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:

1. <https://lists.apache.org/thread/fx278v0twqzxkcts70tc04cp3f8p56pn>
2. <https://lists.apache.org/thread/5zzx8ztwc6tmbw1w80m2pbrp3913l2kl>