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

CERT-MU Vulnerability Note

CERT-MU Vulnerability Note VN-2024-3

Multiple Apache Products Vulnerabilities

Date of Issue: 14.03.2024

Severity Rating: High

Affected Products:

- Apache Tomcat 8.5.0
- Apache Tomcat 9.0.0-M1
- Apache Tomcat 10.1.0-M1
- Apache Tomcat 11.0.0-M1
- Apache Tomcat 8.5.98
- Apache Tomcat 9.0.85
- Apache Tomcat 10.1.18
- Apache Tomcat 11.0.0-M16
- Apache Airflow 2.8.0
- Apache Airflow 2.8.1
- Apache Airflow 2.8.2
- Apache Pulsar 2.11.0
- Apache Pulsar 3.0.0
- Apache Pulsar 3.1.0
- Apache Pulsar 2.10.5
- Apache Pulsar 2.11.3
- Apache Pulsar 3.0.2
- Apache Pulsar 3.1.2
- Apache Pulsar 3.2.0
- Apache Pulsar 2.7.1
- Apache Doris 1.2.7

Description

Apache Tomcat is vulnerable to a denial of service, caused by an incomplete cleanup flaw. By sending specially crafted WebSocket connections, a remote attacker could exploit this vulnerability to increased resource consumption, and results in a denial of service condition.

Apache Airflow could allow a remote authenticated attacker to obtain sensitive information, caused by improper permission validation. By sending a specially crafted request, an attacker could exploit this vulnerability to obtain access resources information, and use this information to launch further attacks against the affected system.

Solution

Users are advised to apply updates to address the vulnerabilities. Before applying the patch, please visit the vendor website for more details:

- https://tomcat.apache.org/
- https://airflow.apache.org/
- https://pulsar.apache.org/
- https://doris.apache.org/

CVE Information

- CVE-2024-23672 CVSS:7.5
- CVE-2024-28746 CVSS:6.5
- CVE-2024-24549 CVSS:7.5
- CVE-2024-28098 CVSS:6.4
- CVE-2024-27317 CVSS:8.4
- CVE-2024-27135 CVSS:8.5
- CVE-2024-27894 CVSS:8.5
- CVE-2022-34321 CVSS:8.2
- CVE-2023-41313 CVSS:7.5

References

- https://www.tenable.com/cve/CVE-2024-23672
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-23672
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-28746
- https://www.tenable.com/cve/CVE-2024-24549
- https://nvd.nist.gov/vuln/detail/CVE-2024-28098
- https://www.tenable.com/cve/CVE-2024-28098
- https://nvd.nist.gov/vuln/detail/CVE-2024-27317
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-27317
- https://nvd.nist.gov/vuln/detail/CVE-2024-27135
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-27135
- https://nvd.nist.gov/vuln/detail/CVE-2024-27894
- https://www.tenable.com/cve/CVE-2024-27894
- https://www.tenable.com/cve/CVE-2022-34321
- https://nvd.nist.gov/vuln/detail/CVE-2023-41313

Report Cyber Incidents

Report cyber security incident on the **Mauritian Cybercrime Online Reporting System (MAUCORS - http://maucors.govmu.org/)**

Contact Information

Computer Emergency Response Team of Mauritius (CERT-MU)
Ministry of Information Technology, Communication and Innovation

Tel: (+230) 4602600
Hotline No: (+230) 800 2378
Gen. Info. : contact@cert.govmu.org
Incident: incident@cert.govmu.org
Website: http://cert-mu.govmu.org
MAUCORS: http://maucors.govmu.org