Apache Tomcat Default Servlet Open Redirect Vulnerability (CSB19-03)

SUMMARY

A vulnerability in Apache Tomcat could allow an unauthenticated, remote attacker to conduct an open redirect attack on a targeted system.

The vulnerability is due to improper validation of URLs by the affected software when the default servlet returns a redirect to a directory. An attacker could exploit this vulnerability by submitting a malicious URL to a targeted system. A successful exploit could cause the redirect to go to any URI of the attacker's choice.

The apache Software Foundation confirmed the vulnerability and released software updates.

ANALYSIS

To exploit this vulnerability, the attacker may need access to trusted, internal networks behind a firewall in order to send a crafted URL to the targeted system. This access requirement may reduce the likelihood of a successful exploit.

IMPACT

Remote attackers redirect users to attacker-controlled websites, tricking users into disclosing sensitive information or executing arbitrary code leading to a system compromise.

SAFEGUARDS

Administrators are advised to:

- **Apply the appropriate software updates;**
- **Allow only trusted users to have network access; and**
- **Monitor affected systems.**

AFFECTED PRODUCTS

Apache Software Foundation Tomcat 7.0.23 to 7.0.90
Apache Software Foundation Tomcat 8.5.0 to 8.5.33
Apache Software Foundation Tomcat 9.0.0.M1 to 9.0.11

FIXED SOFTWARE

The Apache Software Foundation released software updates at the following link:
https://tomcat.apache.org/download-90.cgi#9.0.12

REFERENCE

- https://tools.cisco.com/home/cisco-security/security-advisories-and-alerts/Apache-Tomcat-Default-Servlet-Open-Redirect-Vulnerability
- https://fortiguard.com/encyclopedia/ips/47127
- CVE-2018-11784