August 31, 2023

**Overall rating: High**

**This is a technical bulletin intended for technical audiences.**

## Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of an Apache Tomcat vulnerability. The vulnerability affects Apache Tomcat versions from 11.0.0-M1 through 11.0.0-M10, from 10.1.0-M1 through 10.0.12, from 9.0.0-M1 through 9.0.79 and from 8.5.0 through 8.5.92.

## Technical Details

If the ROOT (default) web application is configured to use FORM authentication, then it is possible that a specially crafted URL could be used to trigger a redirect to an URL of the attacker's choice. URL Redirection to Untrusted Site ('Open Redirect') vulnerability in FORM authentication feature Apache Tomcat. An open redirect is when a malicious website tricks visitors into clicking a link that seems harmless or legitimate but redirects them to a site with malicious intent. This can lead to phishing attacks, data theft, and a general breach of trust. The vulnerability is limited to the ROOT (default) web application. Successful exploitation requires user interaction by the victim.

**Exploitability Metrics**
Attack Vector: Network
Attack Complexity: High
Privileges Required: None
User Interaction: Required

This vulnerability is rated as a **HIGH** risk. A software update exists to address this risk.

## Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have.

## References

- CVE-2023-41080
- Apache Tomcat 9.x vulnerabilities

***Please note that we will be transitioning to a new site on August 31, 2023, where we will post the vulnerability reports.***

You will be able to find all the reports that we have published as well as all future reports here: https://bcgov.sharepoint.com/sites/CITZ-ISB/SitePages/vulnerability-reports.aspx

If you have any questions, please reach out to OCIOSecurity@gov.bc.ca