July 3, 2024

VRM Alert

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of increased risk to unpatched **Apache Tomcat** instances.

Apache Tomcat software is an open-source implementation Jakarta EE platform and is the evolution of the Java EE platform. Apache Tomcat software is developed in an open and participatory environment.

Technical Details

Threat actors can have a variety of reasons to attack your network, gain an information advantage, monetize breached data, or otherwise cause disruptions and harm. **Multiple recent vulnerabilities and increased threat activity have been identified for Apache Tomcat.**

Leveraging recent Apache Tomcat vulnerabilities, a remote attacker could trigger a redirect to an untrusted site, breach information, succeed with a denial-of-service attack, or bypass security restrictions on a targeted system.

The likelihood of an attacker succeeding increases the more patches have not been applied. Vulnerable software can make attacks more effective and harmful. The more damaging an attack is, the greater the return-on-investment generally is to the attacker. Do not depend strictly on network perimeter defences. Patching is an important part of defence-in-depth and helps you to directly keep your systems safe.

Based on the threat level, heightened diligence in patching Apache Tomcat and similar platforms is *very* important right now to your IM/IT ecosystem. If you increase your patching efforts this will bring down your level of vulnerability, and correspondingly your overall level of risk. Additionally, ensure proper configuration of Apache Tomcat during installation e.g. default passwords are changed with the applied updates. Patching means less opportunity for threat actors to be successful and will reduce the likelihood of security incidents occurring. **Important:** Apache Tomcat version 10.1.25 and Apache Tomcat version 9.0.90 are the most recent releases and should be the version(s) you have in current use. If you have a prior version you should work to patch these to current ASAP. *(Note: Apache Tomcat has released 11.0.0-M21 however this is still a beta version.)*

Action Required

- Review installed version of Apache Tomcat (Ensure current patch level, configured securely, and no default credentials.)
- Notify business owner(s).
- Perform mitigating actions, as required. (i.e. patch to the most recent released version).

Please notify VRM with any questions or concerns you may have at VulnerabilityandRiskManagement@gov.bc.ca.

References

- CVE-2024-23672, CVE-2024-24549, CVE-2023-46589
- Apache Tomcat Supported Versions
- Apache Tomcat
- Tomcat 10 Software Downloads
- Tomcat 9 Software Downloads
- VRM Vulnerability Reports