

Overall rating: High



This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware of a regression in the fix for bug 66512 in Apache Tomcat 11.0.0-M5, 10.1.8, 9.0.74 and 8.5.88.

Technical Details

This vulnerability is an attempted solution becoming the source of another problem, the resolution of bug [66512](#), designed to address an entirely different issue. This solution unintentionally sparked a regression, causing the vulnerability: bug [66591](#).

If a response does not have any HTTP headers set, no AJP SEND_HEADERS message is sent. The consequence is that AJP-based proxies, such as mod_proxy_ajp, reuse the response headers from the previous request for the current request resulting in an unintended spillage of information, opens the doors to potential exploitation.

This vulnerability is rated as a **High** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify [VRM](#) with any questions or concerns you may have.

References

- [CVE-2023-34981](#)
- <https://lists.apache.org/thread/j1ksjh9m9gx1q60rtk1sbzmxhvj5h5qz>