

Overall Rating - Critical



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

Summary

The Vulnerability and Risk Management (VRM) Team is aware Apache Shiro, before 1.12.0 or 2.0.0-alpha-3, may be susceptible to a path traversal attack.

Technical Details

Exploitation results in an authentication bypass when used together with APIs or other web frameworks that route requests based on non-normalized requests.

Update to Apache Shiro 1.12.0+ or 2.0.0-alpha-3+

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

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- Ensure mitigation is performed as soon as possible.

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

References

- [CVE-2023-34478](#)
- <http://www.openwall.com/lists/oss-security/2023/07/24/4>
- <https://lists.apache.org/thread/mbv26onkgw9o35rldh7vmq11wpv2t2qk>