January 17, 2024

Overall rating: Critical

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

Summary

The Vulnerability and Risk Management (VRM) Team is aware that Atlassian published a security advisory to address vulnerabilities in the following products:

- Confluence Data Center – multiple versions
- Confluence Server – multiple versions

Successful exploitation of this vulnerability (CVE-2023-22527) can allow an unauthenticated attacker to perform remote code execution.

Technical Details

A template injection vulnerability on out-of-date versions of Confluence Data Center and Server allows an unauthenticated attacker to achieve RCE on an affected version. Customers using an affected version must take immediate action.

Most recent supported versions of Confluence Data Center and Server are not affected by this vulnerability as it was ultimately mitigated during regular updates. However, Atlassian recommends that customers take care to install the latest version to protect their instances from non-critical vulnerabilities outlined in Atlassian's January Security Bulletin.

These vulnerabilities are rated as an overall **Critical** 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-2023-22527
- Atlassian Security bulletin CVE-2023-22527 – Remote Code Execution vulnerability in Confluence Data Center and Confluence Server
- Atlassian Security Advisories