

**Overall rating: Critical**



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

## Summary

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

- Bamboo Data Centre – multiple versions
- Bamboo Server – multiple versions
- Bitbucket Data Centre – multiple versions
- Bitbucket Server – multiple versions
- Confluence Data Center – multiple versions
- Confluence Server – multiple versions
- Jira Service Management Data Center – multiple versions
- Jira Service Management Server – multiple versions
- Jira Software Data Center – multiple versions
- Jira Software Server – multiple versions

## Technical Details

pgjdbc, the PostgreSQL JDBC Driver, allows attacker to inject SQL if using PreferQueryMode=SIMPLE. Note this is not the default. In the default mode there is no vulnerability. A placeholder for a numeric value must be immediately preceded by a minus. There must be a second placeholder for a string value after the first placeholder; both must be on the same line. By constructing a matching string payload, the attacker can inject SQL to alter the query, bypassing the protections that parameterized queries bring against SQL Injection attacks. Versions before 42.7.2, 42.6.1, 42.5.5, 42.4.4, 42.3.9, and 42.2.8 are affected.

### **Exploitability Metrics**

Attack Vector: Network  
Attack Complexity: Low  
Privileges Required: None  
User Interaction: None

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address these risks.

## 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-2024-1597 CVE-2024-21634 CVE-2024-21677
- [Atlassian March 2024 Security Bulletin](#)
- [Atlassian Security Advisories and Bulletins](#)
- [Atlassian Security Advisories and Bulletins](#)