NCC Group
650 California St, Suite 2950
San Francisco, CA 94108
https://nccgroup.com

October 29, 2022

Atlassian Pty Ltd
6/341 George St
Sydney NSW 2000

To Whom It May Concern:

In October 2022, NCC Group conducted a limited security assessment of Atlassian Jira Cloud Prod application. The assessment was designed to support Google's product risk management requirements. For more specific information on scope of the assessment, please see Appendix A.

The assessment objective was to identify critical and high risk security issues within a time-boxed assessment. The assessment combined automated analysis with limited manual penetration testing. In addition, NCC Group reviewed the self-assessment questionnaire completed by Atlassian Pty Ltd. For more information on the testing approach employed, please see Appendix B.

This letter confirms that the assessment of the Atlassian Pty Ltd application has been completed. Upon completion of the assessment, all critical and high risk findings were reported to Atlassian Pty Ltd. At the time of this letter, all critical and high risk findings discovered by the NCC Group assessment have been remediated.

It is important to note that this document represents a point-in-time evaluation of security posture. Security threats and attacker techniques evolve rapidly, and the results of this assessment are not intended to represent an endorsement of the adequacy of current security measures against future threats. This Letter of Assessment necessarily contains information in summary form and is therefore intended for general guidance only; it is not intended as a substitute for detailed research or the exercise of professional judgment. Any mention of effort or length of engagement is not intended to convey coverage; specifically, NCC Group makes no claim of complete coverage of the target(s) of this document. The information presented here should not be construed as professional advice or service.

This testing letter is valid for up to 12 months from the date this letter was issued.

Sincerely,

APPENDIX A - ASSESSMENT SCOPE

This letter addresses the following application:

- Atlassian Pty Ltd + Jira Cloud Prod
- Google Project Number: 118693060927

Application types within the above Project that were assessed included only developer server-resident web applications per the following Google requirements:

- Only apps that accesses Google user data from or through a server are required to get a security assessment
- The Local Data Storage exception specifies that local client applications don't need to undergo a security assessment because data is run, stored, and processed only on the user's device.

The assessment identified the application's use of the following Google OAuth API Restricted Scopes:

Gmail

- https://www.googleapis.com/auth/gmail.modify

APPENDIX B - ASSESSMENT APPROACH

The security assessment included the following activities:

1. **External Network Penetration Testing**
   Identification of potential vulnerabilities in external, internet-facing infrastructure and systems such as the following:
   - Discovery and enumeration of live hosts, open ports, services, unpatched software, administration interfaces, and authentication endpoints lacking MFA
   - Automated vulnerability scanning combined with manual validation
   - Limited credential-guessing against authentication endpoints, directory listings, and other external assets to identify weak credentials
   - Analysis of selected vulnerabilities to estimate exploitability and linkage into attack chaining patterns
2. **Application Penetration Testing** Identification of potential vulnerabilities in the application that accesses Google user data such as the following:
   - Discovery of attack surface, authorization bypass, and input validation issues
   - Automated vulnerability scanning combined with manual validation
   - Technical testing to identify selected software vulnerabilities, insecure configurations, design flaws, and weak authentication, including estimate of exploitability based on observed test results
   - Analysis of selected vulnerabilities to estimate exploitability and linkage into attack chaining patterns
   - Test the ability for users to delete their account and observation/confirmation of external indication that the user or user's content is accessible.
3. **Deployment Review**
   Identification of vulnerabilities in supporting infrastructure such as the following:
   - Analysis of available configuration settings and metadata to build a profile of the supporting environment
   - Analysis of collected information to identify any gaps or deviations from recognized infrastructure security practices
   - Manual examination of configuration settings to locate anomalies and issues such as weak IAM policies, exposed storage containers, poorly defined security groups, insecure cloud services usage, and insecure key management
   - Technical testing as warranted to identify selected vulnerabilities, insecure configurations, design flaws, and weak authentication, including estimate of exploitability based on observed test results
   - Evaluation of OAuth token storage to validate use of encryption, and that encryption keys and secrets are managed appropriately (i.e. stored in a hardware security module or equivalent strength key manager)
   - Evaluation of developer access to the deployment environment to validate use of multi-factor authentication
4. **Policy and Procedure Review**
   Review and examination of information security policies and procedures provided via the Self-Assessment Questionnaire (SAQ) such as the following:
   - Incident response plan: Establishes roles, responsibilities, and actions when an incident occurs
   - Risk management policy: Identifies, reduces, and prevents undesirable incidents or outcomes
   - Vulnerability disclosure program: Provides a means for external parties to report vulnerabilities
   - Information security policy: Establishes rules and guidelines covering the security of information stored digitally

- Privacy User Data Detection: Ensures that users can delete their accounts and related user data by demonstrating an account deletion if relevant