NCC Group
Suite 23.01
Level 23, 45 Clarence Street
Sydney NSW 2000

4th September 2024

Prepared for:

Atlassian
Level 6, 341 George Street
Sydney, NSW 2000, Australia

To Whom It May Concern,

NCC Group were engaged by Atlassian to perform a native application security assessment of the Sourcetree application (part of the Bitbucket Cloud team) to identify security vulnerabilities that may be exploited to compromise ordinary users of the application.

The assessment was conducted between 29/07/2024 and 13/08/2024. The assessment was performed by two consultants, with 10 days for the Windows version and 10 days for the macOS version.

The testing scope and methodology are detailed later in this document.

NCC Group is a global cyber and software resilience business operating across multiple sectors, geographies and technologies. NCC Group is ISO9001 and ISO27001 accredited and a CREST Member Company.

A final report, detailing technical issues and offering remediation advice was provided to Atlassian Pty Ltd at the conclusion of this assessment.

Yours sincerely,

Anthony Caulfield

Associate Director

Testing Scope

Native application security assessment of the Sourcetree application:

- macOS version 4.2.8.
- Windows version 3.4.19.

This was a white-box assessment, with Atlassian providing source code, developer documentation, access to the engineering team, and licenses for professional Integrated Development Environment (IDE) software and static code analysis tools.

Assessment Methodology

The review focused on identifying issues that could be used to compromise users of Sourcetree, including but not limited to:

- Interaction with the underlying operating (such as whether Sourcetree will load libraries or executables from source code repositories).
- Underlying issues with the types of source code repositories Sourcetree can manage, for example, whether it was possible to provide malicious configuration files for Mercurial and Git that lead to code execution.
- Manual source code review, particularly around the web browser URL handler Sourcetree installs.
- Software supply chain issues (are the versions of bundled software up-to-date).
- Automated code analysis with snyk and semgrep.