Brett Fuller

CSD-380 - Assignment 11.2

7/20/2025

Security Controls in Shared Source Code Repositories

What is a code repository?

A code repository is a shared space that allows developers to collaborate on and manage changes to code. In more modern implementations it will typically contain a method for managing working versions through the concept of branches.

Code Repository Risks

Why is it important to secure code repositories?

Code repositories contain a businesses source code which at minimum can contain confidential details about your business and what makes you special. Additionally it can contain a bunch of sensitive data and can even open your business up to additional attack vectors. Aryan Kumar of Encryption Consulting explains these concerns when when they write “These repos have become an easy source of cyber frauds as sometimes attackers can find some sensitive information in codebases like passwords, API tokens, and much more. These code repositories can also lead to supply chain attacks, causing significant financial losses, reputation damage, and business operation disruption.”

Common types of attacks on Code Repositories

1. Typosquatting - Here a name that is slightly different from a popular repository is used in the hopes that the original package will be deprecated and so when someone looks for this functionality in the future they grab the wrong codebase to use as a dependency and gain access to your code base.
2. Credential Theft - If a developer makes a mistake and stores their password data in their code especially in a public repository these credentials can be read and then used as an attack vector.
3. Cloning and Merging - If a code base manager is not paying close enough attention they could inadvertently merge malicious code back into their code base if a bad actor clones, creates a branch, makes bad changes, then makes a pull request for a merger. This technique could allow for the insertion of malicious code.

Security Best Practices

Choose a trustworthy repository

This may seem like simple advice but there are a wide variety of source repositories available at different price points and offered from different providers. Choosing this service from a cheap unknown provider could put your business and your clients at risk. The UK's National Cyber Security Centre gives further guidance on this saying that even with the most trustworthy vendor you should consider "Layering a process of cryptographic signing and verifying code on top of the repository can help to increase confidence that the code has not been tampered with." This extra step means that even if the code repository is compromised these additional layers of security should help inspire trust in the code stored on the repository.

Authorization and Access management

By limiting access to specific users and by applying fine grained access controls preferably based on roles you can limit who has what access to which areas of your code repository. It can limit who has the ability to make changes create branches or merge those branches back into the main branch. Ensuring that only the correct people have these levels of access is critical ensuring your code repository is secure.

Protect Access Credentials

Since many code repositories utilize shared keys to provide authentication make sure to properly train your developers on how to protect them. Gaining access to these keys can be a holy grail for a malicious actor and so at the very least the private keys should be password protected so if they fall into the wrong hands they cannot be easily utilized. Additionally using hardware keys such as FIDO can provide additional layers of security. Finally access keys should be rotated relatively frequently to minimize risk.

Secrets Management

Synk recommends using a secrets management tool to keep your sensitive information outside of your code repository. By utilizing tools to store this information outside of your source control repository you minimize the risk of someone getting access to data that could grant them access to your systems and by utilizing a tool designed specifically for this purpose you are leveraging something that is built to keep sensitive data private.

Handle External Code changes with Care

When working with a public repository where external sources are assisting with your code is extremely important to thoroughly review any proposed changes from external sources. Be extra vigilant in code reviews and consider utilizing tools to scan their code changes against known exploits. The UK's National Cyber Security Centre notes that "attacks could be subtle or disguised. Take extra care if any of this code is automatically run in your build and test infrastructure, as it could be malicious."

Employ External Backups

This is a best practice with pretty much all data in an enterprise and is equally if not more important to be performed against your code repositories. If some disastrous event happened to your code repository and all of your custom code was lost what kind of impact would that have on your business? Even the most trustworthy of code repository providers could fall victim to the wrong kind of attack and having the ability to restore your code somewhere in case of emergency or to provide a comparison should you suspect something is not right in your code base can be critical.

References

Kumar, A. (2024, October 21). *Are Code Repositories Safe for Your Source Code*. Encryption Consulting. Retrieved July 20, 2025, from https://www.encryptionconsulting.com/are-code-repositories-safe-for-your-source-code/

National Cyber Security Centre. (2019, February 20). *Secure development and deployment guidance*. ncsc.gov.uk. Retrieved July 20, 2025, from https://www.ncsc.gov.uk/collection/developers-collection/principles/protect-your-code-repository

Tal, L. (n.d.). *Securing Source Code in Repositories is Essential: How To Get Started*. snyk.io. Retrieved July 20, 2025, from https://snyk.io/articles/securing-source-code-repositories/