Security Controls in Shared Source Code Repositories

Bryan Cabrera, 12/12/2024,
Module 11.2 Presentation

Introduction

- In software development security is of the utmost importance, especially in a world where hacking has been more frequent
- Due to increased hacking attempts there best practices used by development teams in order to protect themselves from unauthorized access, data leaks, and malicious code

Multi-Factor Authentication(MFA)

- Implementing MFA can add an extra layer of protection against any compromised credentials
- MFA prevents unauthorized access even if passwords are leaked
- Requiring MFA for all repository contributors is therefore a recommended best practice

Implement Access Controls

- It is recommended to use role based access control to limit permissions
- This practice reduces the risk of over privileged access and human error
- For a development team it’s recommended to define specific roles like read, write, and admin and assign them properly

Utilize Branch Protection Rules

- Having branch protection rules in place can protect important branches from unauthorized changes
- It’s recommended to set up specific teams for approval and require pull requests before merging
- This practice can prevent both accidental and malicious changes to source code

Mandate Signed Commits

- It’s recommended to have developers sign their commits with private keys to verify authorship
- This practice ensures the authenticity and integrity of commits
- This also helps protect against impersonation and tampering

Automate Security Scans

- It’s recommended to use scanning tools throughout the software development lifecycle
- This way a team can consistently scan for vulnerabilities
- This practice can help identify risks early in the development process

Maintain an Audit Trail/Log

- It’s recommended to use logging features or some kind of monitoring service as part of the development process
- This way you can keep a detailed log of all changes and events
- This practice gives the ability to track and analyze in case breaches occur

Educate Developers

- Naturally a practice that is always recommended is to properly educate developers of security practices that relate to the software development lifecycle
- Doing this reduces the chance of human error and helps improve overall security

Conclusion/ Sources

- In conclusion, implementing these practices reduces security risks involved in the software development process and ensures the integrity of the given repository

Sources: GitOps best practices | Config Sync | Google Cloud
Software security starts with the developer: Securing developer accounts with 2FA - The GitHub Blog
Maintain a secure repository by using GitHub best practices - Training | Microsoft Learn
Quickstart for securing your repository - GitHub Docs