Cloud Software Group Secure Development Lifecycle

Table of Contents

1. Introduction

2. Security Training

3. Planning and Requirements Gathering

4. Threat Modeling

5. Code Review

- A. Manual Code Review
- B. Assisted Code Review(Static Analysis)

6. Supply Chain Security

- A. Third Party Dependency Tracking

7. Security Testing

8. Third Party Penetration Testing

- A. External penetration testing
- B. Bug Bounty Program

9. Product Security Vulnerability and Incident Response Program

10. Product Security Incident Response (PSIRT)

- A. Vulnerability Response

11. Revision History

Secure Development Lifecycle

1. Introduction

Cloud Software Group Product Security team is responsible for the security of all the Cloud Software Group products and services. This team works with the Product Engineering teams to implement the Secure Development Lifecycle (SDL) process that incorporates security throughout the lifecycle of all Cloud Software Group products and services.

This document provides an overview of the security processes for Cloud Software Group products and services. *This information is provided "AS-IS" without warranties of any kind (express or implied) and is subject to change at Cloud Software Group's discretion.*

2. Security Training

Underpinning the SDL process is Secure Development training. We have instituted a continual, level-based security training program for all engineers. This training covers various security elements including threat modeling, secure design principles, secure coding practices, and culminates with Capture the Flag and remediation exercises. As part of the training program, engineers are required to annually revalidate their security awareness knowledge.

3. Planning and Requirements Gathering

Cloud Software Group has adopted Scaled Agile Framework for Enterprise (SAFe) to drive product development. For each development iteration, the Product Security team engages with engineering teams at the planning stage to evaluate the security risks of any new features associated with the release.

4. Threat Modeling

Threat modeling activities are designed to address security design concerns at the initial stage of the development lifecycle. New features, services, and interactions between existing services undergo a threat modeling activity where the product security and engineering teams work together to identify the relevant assets, attack surface, potential threats and corresponding threat vectors.

5. Code Review

A. Manual Code Review

New features go through a code review for any security-sensitive changes, including but not limited to: multi-tenancy flow, memory management, Role-based access control (RBAC), cryptographic code, and authentication/authorization. While performing manual code reviews, the Product Security team focuses on identifying vulnerabilities that might otherwise be missed by Static Application Security Testing (SAST) tools.

B. Assisted Code Review

Beyond the manual code review, Cloud Software Group uses various industry standard SAST tools that are integrated into the pipeline to scan the source code, identify and mitigate any potential vulnerabilities

6. Supply Chain Security

A. Third Party Dependency Tracking

Cloud Software Group uses industry standard tools to perform Software Composition Analysis (SCA). These tools are integrated into build pipelines. This allows us to track the usage of third-party components and to govern open source components vulnerability and licensing policies.

7. Security Testing

The Product Security team performs manual and automated security testing in line with industry best practices for security validation. The Product Security team also performs fuzzing and integrates fuzzing tools with applicable unit test cases to improve coverage for suitable functions and protocols

8. Third Party Penetration Testing

A. External penetration testing

Along with above internal activities, we commission yearly external security assessments and penetration testing engagements by reputable external firms across our product and service portfolio.

B. Bug Bounty Program

Cloud Software Group has a public bug bounty program on HackerOne that provides a pathway for researchers to submit findings in a number of Citrix and NetScaler managed services. We believe the researcher community to be an extension of the security functions performed within the organization and look to engage with the community through regular outreach.

9. Product Security Vulnerability and Incident Response Program

The Product Security function follows industry wide standards for the vulnerability and incident response process to investigate and respond to vulnerabilities that are discovered by external parties

10. Product Security Incident Response (PSIRT)

A. Vulnerability Response

Cloud Software Group takes a comprehensive approach to investigating, addressing and informing customers of known product vulnerabilities. Cloud Software Group also offers multiple avenues to report product vulnerabilities including a continuously monitored, dedicated inbox, and through our active Bug Bounty program.

A customer or security researcher may report a vulnerability through the Trust Center and Report a Security vulnerability. The Vulnerability Response section of the Trust Center includes additional details on the program.

Cloud Software Group publishes security advisories to provide remediation information about security vulnerabilities in customer-managed Cloud Software Group products which have been reported to us through the vulnerability response program.

Further details related to our response process and our approach to vulnerability disclosures can be found on our Trust Center Response Process page.

Cloud Software Group looks to the issues reported or identified through these avenues as feedback to further improve upon the features and components within Cloud Software Group products and services. With this added insight, we can prioritize these components and features for retrospective SDL reviews with a view to use this as an opportunity to identify and implement fixes for the security vulnerabilities.

11. Revision History

Version	Description of Change	Revision Originator	Approvers	Approval & Publication Date
1.0	New SDLC	Product Security	Andy Nallappan, CISO Mohan Sekar, Sr. Director Product Security	Mar 2023
2.0	FY2025 policy Refresh	Product Security	Kumar Palaniappan, CISO Mohan Sekar, Sr. Director Product Security	Feb 2025