citrix

White Paper

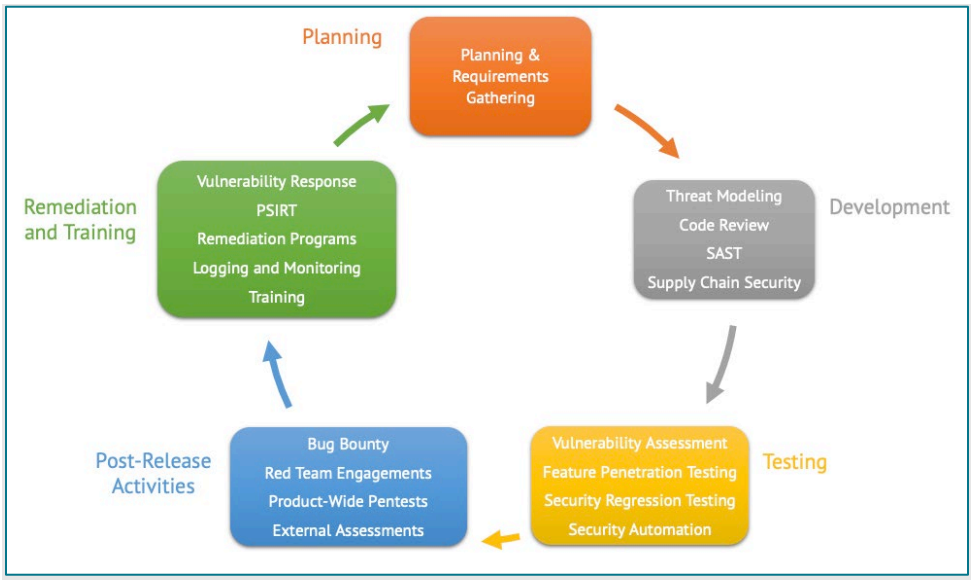
Citrix Security Development Lifecycle

Updated September 2021

Contents

Introduction

Citrix has a dedicated Security Engineering organization responsible for the security of all Citrix products and services. The organization works closely with the Product Engineering Teams to implement the Security Development Lifecycle (SDL) process that incorporates security throughout the lifecycle of all Citrix products and services.



Citrix Security Development Lifecycle (SDL) Process

This document provides an overview of the security work and processes for Citrix products and services.

Citrix Security Development Lifecycle

Planning and Requirements Gathering

Citrix has adopted SAFe (Structured Agile Framework for Enterprise) to drive development. For each quarterly development iteration, the Product Security Engineering (PSEC) and Cloud Security Architecture (CSA) teams engage with engineering teams at the planning stage to evaluate the security risks of any new features associated with the release and initiate the Security Development Lifecycle (SDL) process as applicable.

Additionally, during the planning stage, the security team scopes and obtains commitments from the engineering teams on a prioritized list of new security enhancements and countermeasures.

Threat Modeling

Threat modeling activities are designed to address security design concerns at the application and cloud infrastructure levels. New features, services, and interactions between existing services undergo a threat model where the security and engineering teams work together to identify the assets, attack surface, attackers, and corresponding threats in the system. Threat modeling occurs at the product/application architecture level and at the cloud architecture level. At this stage, the threat model participants ensure that the design conforms to any documented design patterns and standards.

Where threats can be addressed by configuration or code changes, these are planned by the engineering teams. Design changes to address threats are explored between security and engineering teams before they are applied. The outcomes of the design changes are converted into standardized design patterns. Threat models also help identify security tests that validate threat mitigations. These tests are in turn implemented as automated unit or integration tests.

Code Review

Manual Code Review

New features go through an extensive manual code review for any security-sensitive changes, including but not limited to multi-tenancy flow, role-based access control (RBAC), cryptographic code, and authentication/authorization. While performing manual code reviews, the PSEC team focuses on identifying issues that might otherwise be missed by SAST tools, including business logic errors leading to broken authentication and memory corruption.

Assisted Code Review (Static Analysis)

Beyond the manual code review of security-sensitive sections, Static Code Analysis (SAST) tools such as Coverity, Semmle LGTM, SonarQube, .NET Compiler Platform (Roslyn) and PyBandit are integrated into the Continuous Integration pipeline to prevent the addition of new code that may introduce vulnerabilities.

Variant Analysis

In addition to the default rulesets that the SAST solutions provide, the Security Engineering team models incoming vulnerabilities and threats using Semmle CodeQL to find bug variants. The result is a set of custom rules that can be run across an entire project to identify other unknown instances of the same defect.

Supply Chain Security

Third Party Dependency Tracking

Citrix primarily uses Snyk and WhiteSource for Source Composition Analysis (SCA). These tools are available to product build pipelines. This allows Citrix to track the use of third-party components and to enforce vulnerability and licensing policies.

CI/CD Pipeline Security

The Security Engineering organization continually engages with the Infrastructure and Tooling Team to assess and define security requirements for all CI/CD pipelines at Citrix. This includes gap analysis and penetration testing of CI/CD pipeline components and tracking the provenance of all build inputs and outputs.

Vulnerability Scanning

Citrix has an in-house automated scanning framework that aggregates and runs an array of industry standard vulnerability scanners (DAST), like Qualys QualysGuard, Tenable Nessus, Rapid7 Nexpose, BeyondTrust (eEye) Retina, HP Webinspect and IBM AppScan on our products to identify defects and mitigate those issues. These scans are run prior to each release or at least every quarter.

Security Automation

The Security Engineering organization has a Security Automation team with a wide remit. Their activities include enhancing the functionality of testing frameworks and continuously looking at the best tooling to adopt and ensure the security of Citrix products and services. The team also plays a key role in modeling incoming security defects to perform automated variant analysis and find other instances of those defects.

Penetration Testing

Penetration testing is done in multiple phases for each release:

1. The PSEC team runs manual white-box pentest focusing on identifying any OWASP-Top-10 and CWE-Top-25 style defects. The team also looks for defects in business logic flows that can lead to Elevation of Privilege or Cross Tenant bypass attacks. During this phase, we may use tools like application proxies and exploitation frameworks to assist in testing.
2. Citrix also performs fuzzing and integrate fuzzing tools such as Peach and AFL with applicable unit test cases to improve coverage for suitable functions and protocols.
3. For services deployed in the cloud, the CSA team uses a combination of custom, commercial and open-source automated tools, as well as manual assessments, to identify security defects and concerns in the cloud resources used by the service.

Internal and External Engagements

Red Team

Citrix Security Engineering organization's Red Team is responsible for year-round attack simulations on Citrix products, services, networks and security controls.

External Vendor Assessments

As a backstop to these activities, Citrix commissions yearly external security assessments and penetration testing by reputable external firms across its service portfolio.

Bug Bounty Program

Citrix has a public bug bounty program on HackerOne that provides a pathway for researchers to submit findings in a number of Citrix-managed services. Citrix believes the researcher community to be an

extension of the security functions performed within the organization and looks to engage with the community through regular outreach.

PSEC Testing Initiatives

The PSEC team schedules and conducts yearly product-wide penetration tests for Citrix products and services, and updates system-wide product threat models to reflect updates in the design of the product or service.

The results of the Red Team, external vendor assessments, bug bounty program, and PSEC testing initiatives feed directly into Citrix security remediation programs and inform on follow-up activities by the Engineering and Security functions.

Security Training

Underpinning the SDL process is SDL training. Citrix has instituted a continuous security training program for all engineers, split into several levels. The training covers secure coding practices, threat modeling, architecture design, and culminating in capture the flag and remediation exercises. As part of the training program, engineers are required to annually revalidate their security awareness knowledge.

Additionally, the Security Engineering team develops customized and targeted Engineer training that is informed by defect statistics and risk areas.

Security Vulnerability and Incident Response Activities

The external-facing Security Engineering function implements a robust ISO-compliant vulnerability and incident response process to investigate and respond to issues that are discovered by external parties.

Vulnerability Response

Citrix takes a comprehensive approach to investigating, addressing and informing customers of known product vulnerabilities. The product security team follows ISO/IEC standard 29147:2018 concerning disclosure of product vulnerability information. Citrix also offers many ways to report product vulnerabilities, including reporting online or by phone to Citrix support; through a web-based portal on the Citrix Trust Center; and through our Bug Bounty program.

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

Citrix publishes security bulletins to provide remediation information about security vulnerabilities in customer-managed Citrix products which have been reported to Citrix through the vulnerability response program.

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

Product Security Incident Response (PSIRT)

The Product Security Incident Response function responds to and investigates any security events in Citrix's cloud infrastructure that may result in loss of normal functionality, including loss of confidentiality, integrity or availability of an environment or customer information. These are considered critical findings and gaps in the cloud infrastructure and are treated with the highest priority.

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

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, United States