Cloud Software Group Secure Development Lifecycle for Citrix and NetScaler Products & Services

Updated May 2023

Table of Contents

Secure Development Lifecycle

Introduction

Cloud Software Group has a dedicated Product Security team responsible for the security of all Citrix and NetScaler products and services. The team works closely with the Product Engineering teams to implement the Secure Development Lifecycle (SDL) process that incorporates security throughout the lifecycle of all Citrix and NetScaler products and services.

This document provides an overview of the security processes for Citrix and NetScaler products and services. All references to Cloud Software Group processes herein are specific to its Citrix and Netscaler products and services; other Cloud Software Group products and services may follow different processes and customers should refer to the applicable documentation for details.

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.

Security Training

Underpinning the SDL process is Secure Development training. We have instituted a continual security training program for all engineers, split into different levels. The training covers secure coding practices, threat modeling activities, architecture design reviews, 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.

Planning and Requirements Gathering

Cloud Software Group has adopted SAFe (Scaled Agile Framework for Enterprise) 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 and initiate the Secure Development Lifecycle (SDL) process as applicable.

Threat Model

Threat modeling activities are designed to address security design concerns at the initial stage of development lifecycle. New features, services, and interactions between existing services undergo a threat modeling activity 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 participants ensure that the design conforms to any documented design patterns and standards. Where threats can be addressed by configuration or code changes, the engineering team plans these. Design changes to address threats are explored between security and engineering teams before they are applied.

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 Product Security team focuses on identifying issues that might otherwise be missed by SAST (Static Application Security Testing) tools, including but not limited to business logic errors and different types of memory corruption issues.

Assisted Code Review (Static Analysis)

Beyond the manual code review, Cloud Software Group uses various industry standard Static Application Security Testing (SAST) tools that are integrated into the Continuous Integration pipeline to scan the source and identify any potential vulnerabilities.

Supply Chain Security

Third Party Dependency Tracking

Cloud Software Group uses various industry standard tools to perform Software Composition Analysis (SCA). These tools are available to integrate in build pipelines. This allows us to track the use of third-party components and to enforce vulnerability and licensing policies.

CI/CD Pipeline Security

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

Vulnerability Scanning

Cloud Software Group has an in-house automated scanning framework that aggregates and runs an array of industry standard vulnerability scanners and Dynamic application security testing (DAST) solutions on our products to identify defects and mitigate those issues.

Penetration Testing

The Product Security team performs manual white-box penetration testing focusing on identifying OWASP-Top-10 and CWE-Top-25 defects, along with any business logic flaws. During this phase, we may use tools like application proxies and exploitation frameworks to assist in testing. The Product Security team also performs fuzzing and integrates fuzzing tools with applicable unit test cases to improve coverage for suitable functions and protocols. For services deployed in the cloud, the Product Security team uses a combination of custom, commercial and open-source tools, as well as manual assessments, to identify security defects and concerns in the cloud resources used by the service.

Internal and External Engagements

External Vendor Assessments

As a backstop to these activities, we commission yearly external security assessments and penetration testing by reputable external firms across our service portfolio.

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.

Security Vulnerability and Incident Response Activities

The Product Security function implements an ISO-based vulnerability and incident response process to investigate and respond to issues that are discovered by external parties.

Vulnerability Response

Cloud Software Group 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. Cloud Software Group also offers many ways to report product vulnerabilities, including reporting online or by phone to support; through a web-based portal on ourTrust Center; and through our Bug Bounty program.

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

Cloud Software Group publishes security bulletins to provide remediation information about security vulnerabilities in customer-managed Citrix and NetScaler 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 ourTrust Center Response Process page.

Product Security Incident Response (PSIRT)

The Product Security Incident Response function responds to and investigates any security events in our 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.

Cloud Software Group looks to the issues reported or identified through these mechanisms as feedback to further improve upon the features and components within Citrix and NetScaler 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 issues.https://cve.mitre.org/about/faqs.html.

Cloud Software Group