Product Security Incident Response Policy

Purpose

The purpose of this Product Security Incident Response (PSIR) policy is to establish guidelines, responsibilities, and procedures for identifying, evaluating, and mitigating security vulnerabilities and incidents in all Cloud Software Group products. An established response process ensures consistency, accountability, and transparency in the support phase of the secure product lifecycle.

Scope

This policy applies to all Business Units and products under the Cloud Software Group.

Definitions

Incident: A reported event related to a vulnerability or vulnerabilities within a product.

PSIR: Product Security Incident Response.

PSIRT: Product Security Incident Response Team.

Product: Any software developed, produced, or managed by Cloud Software Group

Vulnerability: A weakness in a product that could be exploited to compromise its security. Vulnerabilities can be present in CSG-owned code or in upstream code contained in CSG products.

Zero Day: A software vulnerability unknown to its developers.

Zero Day Attack: The exploitation of a Zero Day vulnerability prior to mitigation.

Responsibilities

PSIR is a cross functional process that involves the Product Security team, the Product Team(s), the Legal team, the Privacy team, and the Support Team. PSIRT follows a standardized incident handling process, which includes the following steps:

Intake: Receive reports of security vulnerabilities and incidents from internal and external sources.

Triage: Prioritize incidents based on severity and potential impact.

Investigation: Incident analysis, root cause identification, mitigation strategy development.

Pre Release: Patch cloud services, coordinate with the team for appropriate vulnerability management, and deploy fixed builds.

Release: Plan and create Security Advisory, inform stakeholders and customers, publish Security Advisory, notify all appropriate parties.

Post-Release: Support Security Advisory via response and escalation subprocesses, update and maintain Security Advisory, track and report trends to Engineering team(s).

Policy

Cloud Software Group shall maintain a PSIR process and PSIRT to facilitate accurate and timely response to reported product vulnerabilities. The PSIRT is responsible for managing the response process from intake to resolution. Cloud Software Group Business Units shall support the PSIRT process by contributing to the verification, triage, and remediation phases.

In order to disclose security vulnerabilities in customer-managed CSG products and provide remediation information to affected customers, the Cloud Software Group PSIRT is responsible for publishing security advisories at https://support.citrix.com/securitybulletins / https://www.tibco.com/services/support/advisories.

Only the PSIRT may publish public information about potential vulnerabilities in Cloud Software Group' products. Other teams may support the PSIRT in publishing such disclosures, but the PSIRT retains ownership of the publishing process.

Cloud Software Group PSIRT Tenets

1. Fair Disclosure

Cloud Software Group adheres to the principle of Fair Disclosure, which ensures that all customers are notified of security vulnerabilities simultaneously. No individual customer, partner, or third party is given advance or preferential access to vulnerability-related information. This principle is fundamental to promoting transparency, consistency, and equitable risk management across our customer base. With an exception of a Pre-Notification program run specific to each Business Units.

2. Fair Remediation

Aligned with the Fair Disclosure principle, Fair Remediation dictates that all customers are granted equal access to vulnerability remediations. Cloud Software Group does not provide early access to security patches, mitigations, or workaround information to any specific customer or entity. All remediations are released as general availability (GA) software updates- accessible to all supported customers under applicable licensing agreements.

3. Disclosure with Remediation

Cloud Software Group's standard practice is to disclose vulnerability information only when effective remediation such as a patch, configuration update, or software upgrade is available. However, in cases where there is evidence of active exploitation or an elevated risk to customer environments, Cloud Software Group, at the discretion of the Product Security Incident Response Team (PSIRT), and in consultation with Legal, may proceed with early disclosure. In such instances, interim guidance and/or compensating controls will be provided to enable customers to take appropriate risk mitigation actions until a full remediation is available.

Responsible Disclosure

- **Vulnerabilities reported through the vulnerability response program:**

  The Cloud Software Group PSIRT will publish security advisories for vulnerabilities in Cloud Software Group products that have been reported by someone outside Cloud Software Group through the vulnerability response program.

- **Vulnerabilities discovered internally:**

  The Cloud Software Group BUs, along with the Product security team and the Legal team, may determine if or when to publish security advisory for internally discovered vulnerabilities in Cloud Software Group products.

- **Third party CVE impact disclosure:**

  Cloud Software Group may also occasionally choose to publish a security article or blog to inform customers of important events affecting Cloud Software Group products, for example, if a critical third-party CVE impacts a CSG product and has gathered significant public attention.

- **Vulnerabilities affecting CSG-managed products or services:**

  Cloud Software Group will not publish a security advisory for vulnerabilities affecting CSG-managed products or services if these can be patched without customers needing to take any action.

- **Vulnerability remediation:**

  Cloud Software Group provides security fixes for all the supported versions of a product **Security releases schedule:**

  Cloud Software Group has adopted a "Patch Tuesday" model for security releases to align with industry practices. This means that, when possible, CSG will publish security bulletins on the second Tuesday of a month. The aims of this are to:

  - Help customers plan to update their products by knowing, in advance, when vulnerabilities will be announced.
  - Reduce negative media attention by announcing vulnerabilities on the same day as other vendors.

  The date of disclosure is typically determined as the Patch Tuesday following the release of a fix in all product versions that have not yet reached EOM. However, this date is at the discretion of the relevant product team, who may choose to delay the disclosure in order of business requirements and risks. Alternatively, if deemed necessary by the BUs and/or Legal, a security bulletin may be released sooner (Out-of-band Releases) without waiting for Patch Tuesday if:

    - A vulnerability is already publicly known or will become publicly known before the next Patch Tuesday
    - A vulnerability is particularly critical and delaying the disclosure would put customers at unnecessary risk of exploitation

  In limited circumstances, including where CSG has observed active exploitation of a vulnerability or where public awareness of a vulnerability could lead to increased risk for CSG customers, a security advisory may be published before a complete set of patches or workarounds have been released in order that we may alert customers to the risk and provide advice on how to mitigate it.

- **Disclosure timeframe:**

  The industry standard timeframe for remediation and disclosure of a vulnerability is 90 days from the date of the vulnerability being reported and the majority of customers and security researchers who report vulnerabilities to CSG expect to receive a fix on or before this date. However, the responsibility for timely fixes lies entirely with the BU and therefore CSG does not commit to disclosing vulnerabilities within 90 days.

- **Zero Day remediation and disclosure:**

  In the event of a Zero Day vulnerability, Cloud Software Group Product Security will take immediate steps to remediate the issue as quickly as possible, and abide by the Cloud Software Group product security vulnerability management standard . Cloud Software Group ensures and maintains fair remediation and a fair disclosure policy at all times. If a previously released CVE is later discovered to have been exploited prior to release, Cloud Software Group PSIRT will update the Security Advisory text to reflect this newly discovered information.