Security response procedure

- Reporting Potential Vulnerabilities in Apache CloudStack
- Security Team
- Scope of ACS Vulnerability Responses
- Procedure for Responding to Potential Security Issues
- Distributor Coordination

Reporting Potential Vulnerabilities in Apache CloudStack

If you've found an issue that you believe is a security vulnerability in a released version of CloudStack, please report it to security@cloudstack.apache.org with details about the vulnerability, how it might be exploited, and any additional information that might be useful.

Upon notification, the ACS security team will initiate the security response procedure. If the issue is validated, the team generally takes 2-4 weeks from notification to public announcement of the vulnerability. During this time, the team will communicate with you as they proceed through the response procedure, and ask that the issue not be announced before an agreed-upon date.

The security team asks that you please do not create publicly-viewable JIRA tickets related to the issue. If validated, a JIRA ticket with the security flag set will be created for tracking the issue in a non-public manner.

Security Team

The PMC has decided to create a "Security Team" for CloudStack. To read more about team membership and activities, please visit CloudStack Security Team

Scope of ACS Vulnerability Responses

The scope of these procedures applies to vulnerabilities found in CloudStack releases 4.0.0-incubating and later.

CloudStack has an history that pre-dates the Apache Software Foundation. This includes the 2.0.x, 2.1.x, 2.2.x, and 3.0.x series of CloudStack releases. Vulnerabilities that are present in only these releases will be addressed by Citrix.

Some vulnerabilities may exist in ASF code releases as well as derivative works or binary distributions. This is discussed in the Distributors section below.

Procedure for Responding to Potential Security Issues

- Upon receiving notice of a potential security issue, a security team member will create a bug to track the investigation, this bug must be flagged as a security issue. Security flag should mean contents of ticket are not visible to non-security team members
- Security team investigates the issue to confirm/deny the presence of a vulnerability within CloudStack
- If the issue is determined not to be a vulnerability the reporter will be notified and the issue will be closed as invalid.
- If issue is confirmed as a CloudStack vulnerability:
  - Security team notifies the Apache Security team (happens automatically - they're on security@ list)
  - Security team creates a Jira issue to document and track the issue, marking it private
  - Security team notifies release manager for target release version
  - Security team assigns a risk rating to the vulnerability using the Common Vulnerability Scoring System
  - Security team works with reporter to get a chance to investigate and mitigate the issue in a timely manner before public announcement. This should be between 15-30 days, depending on the severity and complexity of the issue
  - Security team works with Apache Security Team to reserve a CVE Identifier for future public release
  - Security team works with appropriate code maintainer(s) to create patch to mitigate the issue
  - Testing is conducted to verify patch mitigates issue and does not cause regression errors.
  - Once fix is confirmed, notify release manager to ensure the fix is in the appropriate release.
  - Security team creates a vulnerability announcement
  - Patch is committed to trunk and other supported branches that are affected. The commit should not refer to a particular vulnerability.
  - A new CloudStack release or hotfix is prepared and tested, containing the new security patch.
    - Typically these are narrowly focused maintenance release and do not require official release announcement from ACS marketing. A blog post will be published and user and dev list will be notified.
    - Distributor coordination is implemented to enable a coordinated announcement.
    - Security team posts vulnerability announcement to...
      - CloudStack dev list
      - CloudStack users list
      - CloudStack Security alerts web page
      - The Bugtraq mailing list
  - After announcement, CHANGES and NEWS files need to be updated to reflect the vulnerability and fix. This must happen AFTER the announcement.
  - Also after announcement, modify the Jira ticket so that the issue is now publicly viewable.
- After the vulnerability is addressed, the CloudStack community should review development processes to see how the community can minimize the chance of similar vulnerabilities being introduced in the future.
Distributor Coordination

The CloudStack Security Team will coordinate with members of the Security pre-disclosure list to receive early warning about security issues before they are disclosed to the general public.