CVE Program Policy and Procedure for Disputing a CVE Record

Version: 2.0.0

Approved date: July 2, 2025

Effective date: July 2, 2025

Introduction

This policy and procedure for disputing CVE Records is enforced by [Top-Level Roots (TL-Root)](#) and [Roots](#). This policy applies to all CVE Records that are disputed after July 2, 2025.

Terms and Definitions

Specific terms are defined in the [CVE Program Glossary](#) and are capitalized when used in this document. The following fully capitalized key words explain the requirement levels used in this document:

- MUST: Mandatory
- MUST NOT: Prohibited
- SHOULD: Recommended
- SHOULD NOT: Not recommended
- MAY: Discretionary

CVE Record Dispute Policy and Procedure

The [CVE Program](#) requires all disputes to be initiated and escalated through the appropriate (TL-) Root hierarchy, beginning with the CVE Numbering Authority ([CNA](#)) responsible for the affected scope. If the dispute involves a vulnerability determination outside any CNA's scope, the process may start with a [CNA of Last Resort (CNA-LR)](#).

If a disputing party disagrees with the initial decision of a CNA or CNA-LR, the disputing party MAY escalate the matter to the next level in the hierarchy—either a [Root](#) or [TL-Root](#)—for further review. TL-Roots' decisions are final, except in cases involving cross-hierarchy scope issues.

Disputes spanning multiple hierarchies will be adjudicated by the [Council of Roots](#). Final determinations may uphold the Root or TL-Root decision, concluding the discussion.

The Dispute Resolution Process details can be found below. In cases involving significant cross-scope aspects, relevant parties SHOULD meet to identify the root cause and determine the most appropriate scope, following guidance from the [CVE Program Rules](#).

CVE Records may be disputed for a variety of reasons by various stakeholders participating in the CVE Program. Examples include disputes both before and after the creation of a CVE Record:

1. During Vulnerability Determination

    a. CVE Record Validity: One party contends that a CVE Record should be created, and another party (e.g., a Supplier CNA or CNA-LR) contends that it should not because it is not a valid vulnerability.

    b. Publish as Disputed: While infrequent, some CVE Records are created in disputed status. This occurs when the original reference for the record indicates a bug exists, but there are differences of opinion about whether the bug is a vulnerability based on the CVE Program's definition. The existence of a patch for a bug does not demonstrably prove that a vulnerability exists. In this case, a CNA or CNA-LR MAY decide to assign a [CVE ID](#) and publish a CVE Record with a disputed tag.

2. After CVE Record Creation

    a. CVE Record Validity: A published CVE Record may contain information that a program stakeholder believes is inaccurate. For example, a CNA-LR MAY publish a CVE Record to the [CVE List](#) based on a claim-based vulnerability report submitted by a third party (e.g., an independent researcher). In this example, the Supplier may believe the technology is behaving as intended and no vulnerability exists. When both a claim-based vulnerability report and Supplier assertion of technology behavior are in conflict, and there is insufficient information to demonstrably prove one point of view over another, the CVE Record may be disputed by the Supplier. Third parties MAY also dispute a CVE Record.

    b. CNA Operational Rules Violations: One party contends that the Assignment(s) and Publication(s) of CVE Record(s) are in violation of the CVE Program rules. This covers use cases such as scoping.

    c. Assignment Disagreement: One party contends that a CVE Record(s) should be curated in a manner contrary to the assigning party (e.g., situations where the Assigner and a Researcher disagree on how many CVEs should be assigned to a particular issue).

Process Overview

CNAs, Roots, and TL-Roots MAY serve as CVE Record dispute Adjudicators when necessary. To ensure transparency, each Adjudicator MUST provide a public-facing method for CVE Program stakeholders to initiate and escalate disputes (see CNA Operational Rule 3.2.3.1). Additionally, Adjudicators MUST either host this policy on their public website or provide a direct URL to it, ensuring stakeholders are aware of the dispute resolution process.

CNAs, Roots, and TL-Roots have the flexibility to manage disputes and escalations using methods that best suit their operations, as long as they remain consistent with this policy. TL-Roots, however, hold a unique responsibility to coordinate among themselves when handling disputes involving cross-hierarchy implications.

Dispute and escalation processes must be timely, effective, and aligned with CVE Program rules. Each party involved in a dispute MUST document their rationale, ensuring a structured and transparent escalation process as outlined below.

If the Supplier is a CNA, a CNA-LR MUST not assign a CVE ID or publish a CVE Record without first consulting that CNA. This ensures the supplier CNA has the first right of refusal (see CNA Operational Rule 4.2.1) and helps prevent dispute cascades while maintaining record quality.

Placing the disputed tag allows consumers to determine whether there has been a dispute for a record. If the Adjudicator is unable to place the tag for any reason, the TL-Root or Root MUST update the record on their behalf.

Dispute Resolution Process

1. Initiating a Dispute

    a. The disputing party MUST document and submit their rationale to the Adjudicator, providing supporting evidence such as issue trackers, security policies, or engineering findings.

2. Acknowledgment of Receipt

    a. The Adjudicator MUST acknowledge receipt and initiation of the dispute in writing within three business days.

3. Tagging the CVE Record

    a. If the dispute appears potentially legitimate, the Adjudicator MUST tag the CVE Record as disputed and provide a reason in the CVE Record while the process is ongoing.

b. If the dispute is later deemed invalid or resolved, the Adjudicator MUST remove the disputed tag and reason.

4. Review and Stakeholder Engagement

a. The Adjudicator MUST review the rationale and engage relevant stakeholders as necessary to fully understand the dispute.

5. Adjudication and Decision Timeline

a. The Adjudicator MUST apply CNA Operational Rules to assess the dispute and reach a decision within five business days after the three-day acknowledgment period.

b. If additional time is required, the Adjudicator MUST notify all parties.

c. If an extension exceeds 15 business days, any involved party MAY escalate the dispute to the Root, who will coordinate with the Adjudicator to establish an appropriate resolution timeline.

Dispute Outcomes

1. Valid Dispute

a. The Adjudicator MUST make reasonable efforts to notify all relevant parties in writing and MUST modify (or initially publish) the CVE Record accordingly.

b. If the disputing party agrees with the action, no escalation is required.

c. If the disputing party disagrees, they MAY escalate the issue.

2. Invalid Dispute

a. The Adjudicator MUST make reasonable efforts to notify the disputing party in writing that no changes will be made to the CVE Record.

b. The disputing party retains the right to escalate the issue.

3. Dispute Reconsideration

a. Any party MAY provide additional correspondence to support their position if they believe the decision was incorrect.

b. The Adjudicator MAY choose not to respond, taking no further action, effectively leaving the case closed.

c. The Adjudicator MAY review and revise the decision.

d. Reconsideration criteria could include but is not limited to the severity of the vulnerability and whether the CNA's publication practices align with industry expectations.

e. If the dispute is escalated, the Root or TL-Root MUST follow the same procedure.

f. Regardless of the outcome, the Root or TL-Root MUST inform all parties about the dispute escalation process by referencing this policy.

4. Final Dispute Tagging

In cases where the dispute is determined not valid by the final Adjudicator, the CVE Record MUST be updated to remove the "disputed" tag in a timely manner.

5. No Resolution Reached

It should be noted that not all disputes require a resolution. There are cases where there will be ongoing disputes after a review. In that case, the CVE Record will continue to be tagged as disputed and will continue to provide a reason for the dispute.