CVE® Numbering Authority (CNA) Operational Rules

Version 4.0

Effective August 8, 2024

Approved by CVE Board on May 8, 2024

Table of Contents

1 Introduction

1.1 Background

The Common Vulnerabilities and Exposures (CVE) Program is a voluntary, international, community-driven effort to identify, define, catalog, and share information about Publicly Disclosed cybersecurity Vulnerabilities. A CVE Identifier (CVE ID) and corresponding CVE Record enable multiple parties to discuss and share information with confidence that they are referencing the appropriate Vulnerability. This Vulnerability identification capability is fundamental to global Vulnerability management.

Within the CVE Program, a CVE Numbering Authority (CNA) is an organization authorized to assign CVE IDs and publish CVE Records, ideally as part of the initial Public Disclosure of a Vulnerability. Benefits of participating in the CVE Program as a CNA include the ability to Publicly Disclose Vulnerabilities with pre-assigned CVE IDs and the first opportunity to assign CVE IDs for Vulnerabilities within the CNA's Scope Definition. In addition to assigning CVE IDs, CNAs also create and publish information about the identified Vulnerability in its associated CVE Record.

Many CNAs are Suppliers who assign CVE IDs to and publish CVE Records for Vulnerabilities affecting Products owned, developed, or maintained by the Supplier. Examples of CNAs include:

- Software and hardware Suppliers, including product security incident response teams (PSIRTs)
- Open source software projects, maintainers, and foundations
- Service providers
- Vulnerability researchers
- National computer security incident response teams (CSIRTs)
- Vulnerability coordinators
- Vulnerability databases
- Bug bounty providers

1.2 Adherence to CVE Program Policies and Rules

To participate in the CVE Program, CNAs:

1.2.1 MUST agree and adhere to program policies, guidance, responsibilities, and rules, which are listed in the Rules & Policies section of the Resources page, and

1.2.2 MUST operate under the CVE Terms of Use License, and

1.2.3 MUST comply with the CNA Operational Rules defined in this document.

1.2.3.1 Serious or repeated failure to adhere to these rules MUST be reviewed by an appropriate Root. The CVE Board MAY revoke CNA status.

1.2.3.2 An appropriate Root MUST notify a CNA of any infractions that initiate a review.

1.3 Document Purpose

The purpose of this document is to define the rules and practices CNAs, CNA-LRs, and Roots are expected to follow. This document defines operational rules for:

- Administering CNAs
- Defining CNA scope
- Identifying and determining Vulnerabilities
- Assigning CVE IDs
- Managing and publishing CVE Records

1.4 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

1.5 Other Useful Information

To successfully interpret and follow the CNA Operational Rules, it is necessary to read the entire document comprehensively. The correct interpretation of an individual rule may require context provided by other rules. It may be necessary or useful to consult other sources of information, including but not limited to:

- CVE Program Glossary
- CVE Program Policy and Procedure for Disputing a CVE Record
- End of Life Vulnerability Assignment Process
- CVE Program Policy and Procedure for Inactive CNAs
- CVE Record Lifecycle
- CVE Program Professional Code of Conduct

2 Managing the CNA Operational Rules

The CNA Operational Rules are managed, maintained, and approved by the CVE Board.

2.1 Changes to the CNA Operational Rules

2.1.1 Changes to the CNA Operational Rules are subject to approval by the CVE Board.

2.1.2 Changes MAY be proposed by CVE Program participants (CNAs, CNA-LRs, Roots, TL-Roots, the Secretariat, the Board, working groups) to the Secretariat who MUST present them to the Board.

2.1.3 When processing changes, the CVE Board MUST consider input from and impact to CVE Program participants, MUST provide advance notice, and MUST provide the opportunity to review and comment.

2.1.4 Changes MUST be considered, decided, and documented in a transparent process.

2.1.5 Changes MUST NOT be applied retroactively to existing CVE ID assignments and published CVE Records.

2.2 Root Additions to the CNA Operational Rules

2.2.1 A Root MAY make additions to the CNA Rules. The additions MUST only apply to CNAs within the Root's hierarchy. The additions MUST NOT conflict with the primary CNA Operational Rules described in this document.

2.2.2 The Root MUST obtain approval for any such additions from the appropriate TL-Root.

2.3 Exceptions to the CNA Operational Rules

2.3.1 A CNA MAY request an exception to the CNA Operational Rules from the CVE Board. The CNA MUST provide justification for the exception.

2.3.2 Only the CVE Board has authority to approve exceptions to the CNA Rules on a case-by-case basis.

2.3.3 The Secretariat MUST document any exceptions approved by the CVE Board.

2.4 CNA-LR Operational Rules

CNA-LRs typically have broader scopes than CNAs. This can contribute to high rates and volumes of CVE ID assignment requests to a CNA-LR. CNA-LRs:

2.4.1 MUST follow the CNA Operational Rules, and

2.4.2 MUST follow any additional rules specified by their TL-Root (see 2.2), and

2.4.3 MAY limit effort to optimize service given resource constraints, for example, by not notifying Suppliers who are not CNAs (4.3.2) and by not publishing advisories or other information about vulnerabilities (4.5.2.1) for assigned CVE IDs.

3 CNA Administration

3.1 CNA Scope Definition

CNAs describe which Vulnerabilities they assign CVE IDs and publish CVE Records for using a Scope Definition. For Supplier CNAs, scope is often defined in terms of Products owned, developed, or maintained by the CNA. For Vulnerability research or coordination CNAs, scope is often defined in terms of Vulnerabilities that are researched or coordinated by the CNA. In all cases, the CNA with the most appropriate scope should have the first opportunity to assign (see 4.2.1). The CNA with the most appropriate scope is often, but not always, the Supplier of the Product in question. It is important to define scopes and manage scope overlap in order to minimize duplicate assignments and other confusion.

3.1.1 CNAs MUST develop, document, and operate within a Scope Definition that describes the types of Vulnerabilities for which the CNA will assign CVE IDs.

3.1.1.1 The Scope Definition is initially established during the CNA on-boarding process and MUST be completed and approved prior to a new CNA being authorized.

3.1.1.2 The CNA MUST obtain approval for the Scope Definition from their Root or TL-Root. The Scope Definition is subject to review and final approval by the Secretariat. Approved Scope Definitions MUST be published in the List of Partners.

3.1.2 A CNA MAY change their Scope Definition. Changes are subject to approval as specified in 3.1.1.2.

3.1.3 Supplier CNAs SHOULD define Scope in reasonably broad terms, such as:

- All of a Supplier's Products:
  Example: "Supplier X's products only"
- A list of specific Products:
  Example: "Supplier Y's Remote Desktop Manager and Server products only"
- A list of covered and not covered Products:
  Example: "All of Supplier Z's Products except for Remote Desktop Manager and Server products"
- Specifying scope for End-of-Life (EOL) Products:
  Example: "Supplier A's supported Products and End-of-Life products"

3.1.4 For Scope Definitions based on Products, the Scope Definition MUST include a covered set of Products and MUST NOT only list non-covered items.

3.1.5 Scope Definitions SHOULD be general enough to cover the evolving set of Products while being specific enough to understand the assignment boundaries for the CNA.

3.1.6 When appropriate, Scope Definitions SHOULD include Product and brand names that are supported during and shortly after mergers and acquisitions, for example: "All XYZ (formerly A and B) Products."

3.1.7 CNAs SHOULD update Scope Definitions for significant changes in coverage, for example, the introduction of new Products, Product lines, brands, mergers, or acquisitions that are not covered by an existing Scope Definition. CNAs MAY also change Scope Definitions due to process changes in, for example, EOL handling or Vulnerability reporting.

3.1.7.1 CNAs SHOULD NOT update Scope Definitions for minor changes in coverage, for example, new Products or Product versions that are already covered by an existing, sufficiently broad Scope Definition.

3.1.8 Research or coordination CNAs SHOULD define Scope in terms of Vulnerabilities that are researched or coordinated by the CNA, unless the Vulnerabilities are covered by a CNA with more specific scope.

- Example: "…and for Vulnerabilities discovered by Organization Y, if the Product is not in another CNA's scope."
- Example: "We will assign CVE IDs for Products that we are researching or coordinating unless they are in another CNA's scope."

3.1.9 When appropriate and clarifying, and subject to scope approval as specified in 3.1.1, a CNA MAY link to additional information to support its Scope Definition. For example:

- "Supplier Z's Products listed on https://supplier.example.com/security/cvescope"

3.1.10 CNA Scope Definition disputes MUST initially be handled at the Root, TL-Root, or Council of Roots level. If the dispute cannot be resolved at these levels, then the dispute MUST be brought to the Secretariat who MUST inform the CVE Board. The CVE Board then makes the final decision.

3.1.11 Scope Definitions for End-of-Life (EOL) Products

3.1.11.1 A CNA MAY specify in its Scope Definition whether and how the CNA assigns CVE IDs for EOL Products. See 4.2.17.5.

3.1.12 Multiple Program Roles

3.1.12.1 Multiple roles exist in the CVE Program. Organizations with multiple CNAs or CNA-LRs MUST specify individual Scope Definitions for each CNA or CNA-LR. CVE Program roles are documented in the List of Partners. For example, MITRE currently acts as the Secretariat, a TL-Root, and a CNA-LR.

3.2 CNA Administration

3.2.1 Administration Interfaces

3.2.1.1 CNAs MUST use services and mechanisms specified by the CVE Program to manage CNA accounts and other organizational information.

3.2.1.2 CNAs MUST disable or deactivate or otherwise manage inactive user accounts in a timely manner, which the Secretariat MAY determine.

3.2.2 Administrative Point of Contact

3.2.2.1 CNAs MUST provide administrative point of contact (POC) information to their Root, TL-Root, and the Secretariat. The administrative POC will be used to contact the CNA for administrative, governance, and operational reasons, including important or urgent issues requiring escalation.

3.2.2.2 The administrative POC MUST include both email addresses and phone numbers and MAY include additional contact methods.

3.2.2.3 The administrative POC MAY be shared with CVE Program participants when needed. The administrative POC information MUST not be made available to the general public and MUST NOT be shared outside of CVE Program without prior approval by the CNA.

3.2.2.4 CNAs MUST maintain current administrative POC information in the event of changes in personnel or availability. CNAs SHOULD provide at least two individuals or addresses for the administrative POC.

3.2.2.5 The administrative POC MUST respond in a timely manner. Automated responses do not qualify as “a timely manner.”

3.2.3 Public Point of Contact

3.2.3.1 CNAs MUST provide public POC information that is published in the List of Partners. The public POC is used for requests related to CVE ID assignment, CVE Record content, and other CVE-related issues.

3.2.3.2 CNAs MUST inform their Root, TL-Root, and the Secretariat when public POC information changes.

3.2.4 Availability and Responsiveness

3.2.4.1 Subject to their respective CNA Scope Definitions, CNAs MUST respond in a timely manner to CVE ID assignment requests submitted through the CNA's public POC.

3.2.4.2 CNAs SHOULD document their expected response times, including those for the public POC.

3.2.4.3 CNAs are subject to the CVE Program Policy and Procedure for Inactive CNAs.

3.2.4.4 CNAs MUST be aware of CVE Program communications through official mechanisms defined by the Program, currently, the CVE CNA Discussion mailing list.

3.2.5 Changes to CNA Status

3.2.5.1 When a merger, acquisition, or other organizational change materially affects a CNA, the CNA's Root SHOULD review the CNA's Scope Definition and capabilities. The Root MAY decide to re-train or re-qualify the CNA and the CNA may request assistance from the Root.

3.2.5.2 As noted in 1.2.3.1, serious or repeated failure to adhere to the CNA Operational Rules MUST be reviewed by the appropriate Root. The CVE Board MAY revoke CNA status.

3.2.6 CVE ID Assignment and Vulnerability Disclosure

The CVE Program itself does not follow or require a specific Vulnerability disclosure policy. CNAs and other CVE Program participants operate under a variety of Vulnerability disclosure policies. Some CNAs do not directly participate in Vulnerability disclosure. Common elements of a Vulnerability disclosure policy include:

- Making reasonable attempts to notify Suppliers
- Providing good-quality Vulnerability reports
- Describing Vulnerability report intake processes
- Describing bug bounty policies and processes, if applicable
- Setting expectations for response times
- Providing an embargo period during which the Vulnerability will not be Publicly Disclosed while the Supplier develops a Fix or mitigation
- Coordinating the Public Disclosure date
- Publishing Vulnerability advisories

3.2.6.1 CNAs MUST publish guidance that describes how the CNA assigns CVE IDs and publishes CVE Records within the context of Vulnerability disclosure.

3.2.6.2 CNAs MUST provide a URL to their CVE ID assignment and Vulnerability disclosure policies that will be included in the List of Partners.

3.2.6.3 CNAs MAY require CVE ID assignment to be made using specific processes or mechanisms. Such processes or mechanisms MUST NOT conflict with the CNA Operational Rules.

3.2.6.4 A CNA’s Vulnerability disclosure policy MUST NOT prevent the CNA from following the CNA Operational Rules.

4 CNA Operational Rules

4.1 Vulnerability Determination

CVE identifies technical, cybersecurity Vulnerabilities. The CVE Program Glossary defines a Vulnerability as:

> an instance of one or more weaknesses in a Product that can be exploited, causing a negative impact to confidentiality, integrity, or availability; a set of conditions or behaviors that allows the violation of an explicit or implicit security policy.

Vulnerability reports sometimes confuse or conflate multiple Vulnerabilities or "Vulnerability-like" issues. Consistent Vulnerability determination reduces the likelihood of missing or duplicate CVE ID assignments. CNAs are expected, when necessary, to use experience and judgment (4.4) to determine the existence of one or more Vulnerabilities. Roots and TL-Roots may provide additional guidance to their CNAs to supplement the Vulnerability determination (4.1) and CVE ID assignment rules (4.2) specified in this document. This allows the CVE Program to adapt to definitions used in different industries, technologies, legal regimes, and cultures. Prior to assigning CVE IDs, CNAs MUST follow the rules and guidance in this section to determine the existence, scope, and extent of Vulnerabilities.

4.1.1 If a Supplier determines that a Vulnerability exists in a Product, then CNAs SHOULD agree with this determination.

4.1.2 Conditions or behaviors that do not lead to a security impact SHOULD NOT be determined to be Vulnerabilities. Examples of security impacts include an increase in access for an attacker, a decrease in availability of a target, or another violation of security policy.

4.1.3 Well-documented or commonly-understood non-default configuration or runtime changes made by an authorized user SHOULD NOT be determined to be Vulnerabilities.

4.1.4 Insecure default configuration settings SHOULD be determined to be Vulnerabilities.

4.1.5 Physical attacks SHOULD NOT be determined to be Vulnerabilities unless there is a specific security feature, supported claim, or policy that defends the Product against the physical attack.

4.1.5.1 A Vulnerability SHOULD be determined to exist if, for example, a Product deletes user data after a number of failed login attempts or only boots with known good components, and such defenses can be reduced or bypassed.

4.1.5.2 Physical theft, damage, or destruction are not by themselves cybersecurity Vulnerabilities. CNAs SHOULD NOT determine physical access to a processor, memory, bus, or other hardware component to be a cybersecurity Vulnerability.

4.1.6 Brute-force denial-of-service and brute-force resource exhaustion attacks, for example, high-rate or high-bandwidth denial-of-service attacks or jamming radio frequency spectrum,

SHOULD NOT be determined to be Vulnerabilities. Failure to implement common defenses against such attacks MAY be determined to be a Vulnerability (for example, an instance of CWE-770).

4.1.7 Detection bypass attacks SHOULD NOT be determined to be Vulnerabilities unless, for example, a Product explicitly claims to detect a specific pattern and fails to do so.

4.1.8 General purpose deliberately malicious code MUST NOT be determined to be a Vulnerability.

4.1.9 Products that have been modified to become malicious, for example, trojan horses, backdoors, or similar supply chain compromises, MAY be determined to be a Vulnerability.

4.1.10 To help determine whether separate Vulnerabilities exist, CNAs SHOULD consider whether the Vulnerabilities are Independently Fixable.

4.1.11 Interdependent conditions that cause a Vulnerability SHOULD be determined to be one Vulnerability. For example, if a buffer overflow occurs only when an integer overflow occurs, CNAs SHOULD determine these two conditions to be one Vulnerability.

4.1.12 The act of updating Product dependencies MUST NOT be determined to be a Vulnerability, regardless of whether the dependencies have Vulnerabilities. For example, updating a library to address a Vulnerability in that library MUST NOT be determined to be a new Vulnerability in a Product that uses the library, and a Vulnerability advisory for the Product SHOULD reference the CVE ID for the Vulnerability in the library. See 4.2.13.

4.1.13 Sociotechnical and other changes over time MAY be determined to be new Vulnerabilities or types of Vulnerabilities. Examples include advancements in computing power that make existing cryptographic algorithms insecure (such as CVE-2004-2761, CVE-2020-5229, instances of CWE-328) and changes in attitudes about the use of plain-text protocols (such as CVE-2020-29380, an instance of CWE-319). CNAs are expected to exercise judgment as described in 4.4. See also 4.2.8 and 4.4.4.

4.1.14 When useful or necessary to clarify Vulnerability determination decisions and CVE ID assignments, CNAs SHOULD explain relationships between CVE IDs and Fixes, Vulnerability determination decisions, and CVE ID assignment decisions. CNAs MAY explain these relationships using CVE Record descriptions and references. Note that CNAs are expected and required to exercise judgment (4.4), which is often necessary for complicated CVE ID assignments.

4.2 CVE ID Assignment

After determining that one or more Vulnerabilities exist, CNAs should follow the guidance in this section to assign CVE IDs.

4.2.1 First Refusal

CVE ID assignment follows a “right of first refusal” model.

4.2.1.1 The CNA with the most appropriate scope MUST be contacted and given the first opportunity to assign. In many cases, this CNA is the Supplier of the Product in question.

4.2.1.2 For Publicly Disclosed Vulnerabilities, if the CNA with the most appropriate scope:

1. preemptively documents that it will not assign, or
2. responds within 72 hours that it will not assign, or
3. does not respond within 72 hours,

then an appropriate Root MUST make a Vulnerability determination. If the Root determines that one or more Vulnerabilities exist, the Root MUST direct a CNA-LR or another CNA with appropriate scope to assign as quickly as possible and no later than 72 hours after becoming aware of the first refusal. Ownership of the CVE Record MAY be transferred.

4.2.1.3 For Vulnerabilities that are not yet Publicly Disclosed, if the CNA with the most appropriate scope decides not to assign, the party requesting assignment MUST follow the dispute resolution guidance in 4.6.

4.2.2 Primary Assignment

4.2.2.1 CNAs SHOULD assign a CVE ID if:

1. the CNA has reasonable evidence to determine the existence of a Vulnerability (4.1), and
2. the Vulnerability has been or is expected to be Publicly Disclosed, and
3. the CNA has appropriate scope (3.1).

4.2.2.2 CNAs SHOULD Publicly Disclose and assign a CVE ID if the Vulnerability:

1. has the potential to cause significant harm, or
2. requires action or risk assessment by parties other than the CNA or Supplier.

4.2.2.3 CNAs MAY Publicly Disclose Vulnerabilities for other reasons.

4.2.3 CNAs MUST NOT consider the type of technology (e.g., cloud, on-premises, artificial intelligence, machine learning) as the sole basis for determining assignment.

4.2.4 If a CNA assigns a CVE ID, the Vulnerability MUST be Publicly Disclosed by the CNA or another party, or the CNA MUST reject the CVE ID.

4.2.5 CNAs MUST NOT assign CVE IDs for Vulnerabilities the CNA does not intend to Publicly Disclose unless the Vulnerabilities are already or are expected to be Publicly Disclosed.

4.2.6 CNAs SHOULD assign different CVE IDs to separate Vulnerabilities, as determined using the guidance in 4.1.

4.2.7 CNAs SHOULD assign CVE IDs to Vulnerabilities, not Fixes for Vulnerabilities. CNAs SHOULD assign CVE IDs whether or not a Fix is available.

4.2.8 CNAs MAY determine that residual insecurity left by an incomplete Fix is a new Vulnerability and MAY assign a new CVE ID or MAY use an existing CVE ID.

4.2.9 When useful or necessary to clarify CVE ID assignments, CNAs SHOULD follow the guidance in 4.1.14.

4.2.10 CNAs SHOULD NOT assign CVE IDs to Vulnerabilities in Products that are not and were never publicly available.

4.2.11 CNAs SHOULD assign different CVE IDs to different, Independently Fixable Vulnerabilities.

4.2.12 If a CNA is uncertain whether two issues are Independently Fixable, then the CNA SHOULD assign a single CVE ID.

4.2.13 If multiple Products are affected by the same Independently Fixable Vulnerability, then the CNA:

1. MUST NOT assign more than one CVE ID if the Products are vulnerable because they share the vulnerable code. The assigned CVE ID will be shared by the vulnerable Products.
2. SHOULD assign different CVE IDs if the Products do not share vulnerable code.
3. SHOULD assign different CVE IDs if the CNA is uncertain whether the Products share vulnerable code.

4.2.14 If a Product is affected by a Vulnerability because it uses the functionality or specification of another Product, then a CNA:

1. MUST assign a CVE ID to each known vulnerable implementation if there is a secure way of using the functionality or specification.
2. MUST assign a single CVE ID if there is no option to use the functionality or specification in a secure way.
3. SHOULD assign different CVE IDs to each known vulnerable implementation if the CNA is uncertain whether there is a secure way.

4.2.15 CNAs MUST NOT assign a different CVE ID to a Vulnerability that is fully interdependent with another Vulnerability. The Vulnerabilities are effectively the same single Vulnerability and MUST use one CVE ID.

4.2.16 Multiple CNAs With Overlapping Scopes

CNAs are constrained to assigning CVE IDs to Vulnerabilities within their Scope Definitions. Sometimes, Scope Definitions overlap. Examples include research CNAs who discover the same Vulnerability at the same time and Supplier CNAs whose Products use the same vulnerable library and may be involved in a multi-party coordinated Vulnerability disclosure

process. In cases like these, the rules below clarify which CNA assigns the CVE ID. Scope Definition is discussed in 3.1.

4.2.16.1 CNAs MUST NOT assign CVE IDs to Vulnerabilities outside of their scope.

4.2.16.2 CNAs SHOULD assign CVE IDs within their scope.

4.2.16.3 If a Vulnerability that has not yet been Publicly Disclosed falls within the scope of multiple CNAs, then the CNAs who are aware of the Vulnerability SHOULD work together to assign CVE IDs.

4.2.16.4 If multiple CNAs with overlapping scopes are coordinating the Public Disclosure of a Vulnerability, those CNAs SHOULD work together to assign CVE IDs.

4.2.16.5 If a Vulnerability falls within the scope of multiple CNAs, and the CNAs cannot resolve the assignment decision themselves, the decision about which CNA assigns the ID MUST be made by the lowest level organization (Root, TL-Root, Council of Roots) that is shared by the CNAs.

4.2.16.6 If a Supplier CNA becomes aware of a Vulnerability in an upstream dependency used by the Supplier CNA, they MUST notify and defer first-refusal CVE ID assignment to the upstream Supplier of the dependency, if the upstream Supplier is a CNA.

4.2.17 End-of Life Products

4.2.17.1 CNAs SHOULD assign CVE IDs for EOL Products that no longer receive Fixes. CNAs MUST tag CVE Records that only cover Products that no longer receive Fixes as "unsupported-when-assigned." See also 5.1.11.

4.2.17.2 TL-Roots MAY define CVE ID assignment process for EOL Products within the TL-Root's hierarchy. Such processes MUST NOT conflict with the CNA Operational Rules and the End of Life Vulnerability Assignment Process unless the CVE Board approves an exception.

4.2.17.3 CNAs MUST follow their TL-Root's documented process. If one does not exist, CNAs MUST follow the guidance in the End of Life Vulnerability Assignment Process.

4.2.17.4 Subject to TL-Root EOL processes and the End of Life Vulnerability Assignment Process, if a CNA specifies that it does not assign CVE IDs for Vulnerabilities in EOL Products, then other CNAs with appropriate scope MAY assign. To minimize duplicate assignments for Publicly Disclosed Vulnerabilities, CNAs SHOULD defer assignment to Roots and Roots SHOULD direct CNA-LRs to assign. See also 4.2.1.

4.2.17.5 CNAs SHOULD publicly document how they assign CVE ID for EOL Products. CNAs MAY do this in their Scope Definition (see 3.1.11).

4.2.17.6 If a CNA does not publicly document how they assign CVE IDs for EOL Products, then it should be assumed that the CNA will handle assignment similarly for EOL Products and non-EOL Products.

4.2.18 CNAs MUST NOT assign CVE IDs for Vulnerabilities that have been deliberately implemented for educational and research purposes, for example, in Products such as OWASP WebGoat.

4.2.19 As part of handling CVE ID assignment requests, CNAs SHOULD ask requesters if they have already requested an assignment from another CNA with appropriate scope. If so, the CNA SHOULD defer assignment to the initial CNA, refer the requester back to the initial CNA, or otherwise coordinate with the initial CNA.

4.2.20 To help minimize duplicate assignments, CNAs SHOULD consider coordinating with an appropriate Root or CNA-LR before assigning CVE IDs for Publicly Disclosed Vulnerabilities. See 4.2.1.2 for more specific guidance.

4.3 Notification

4.3.1 When a CNA becomes aware of a non-public Vulnerability report, CVE ID request, or CVE ID assignment that is only covered by the Scope Definition of a different CNA, the first CNA SHOULD either refer the reporter or requester to or attempt to notify the appropriate CNA.

4.3.2 If a CNA is considering an assignment, and the CNA is not the Supplier of the vulnerable Product, then the CNA SHOULD make a reasonable and good faith effort to notify the Supplier. For example, if an operating system Supplier discovers a Vulnerability in a library from an upstream Supplier, in addition to assigning the CVE ID to the upstream Vulnerability, the operating system Supplier SHOULD attempt to notify the upstream library Supplier. This reduces duplicate CVE ID assignments and helps alert others that may be affected by the Vulnerability.

4.3.3 When a Vulnerability is reported to a CNA and the CNA assigns a CVE ID to the Vulnerability, the CNA MUST provide the CVE ID to the reporter.

4.4 CNA Judgment

Within the context of these rules, CNAs are expected to exercise discretion and judgment, especially when making complicated Vulnerability determination (4.1) and CVE ID assignment (4.2) decisions. Specific examples include:

- Sufficient and reasonable evidence of Vulnerability
- Vulnerability abstraction, including the interpretation of Independently Fixable
- Number of Vulnerabilities and CVE ID assignments
- Rejecting CVE IDs or making other abstraction or assignment changes
- Violation of an explicit or implicit security policy or claim
- Potential for a Vulnerability to cause significant harm
- Requirement for action or risk assessment by parties other than the CNA
- How to resolve disputes and when to escalate

4.4.1 Disagreements with a CNA's decision or judgment, including whether and how to assign CVE IDs, MUST follow the CVE Program Policy and Procedure for Disputing a CVE Record.

4.4.2 CNAs SHOULD consult others (such as peer CNAs, CNA-LRs, Roots, and parties with knowledge of the Vulnerability) when making a decision involving significant or unusual judgment.

4.4.3 If, after a reasonable good faith effort, the CNA cannot make a clear decision, the CNA SHOULD err on the side of assignment and SHOULD assign CVE IDs. Doing so allows CVE users to identify and discuss the “Vulnerability-like” issue.

4.4.4 If consensus around a “Vulnerability-like” issue develops, the CVE Program MUST consider whether and how to update these rules and other guidance.

4.5 CVE Record Management

This section specifies actions related to publishing and managing CVE Records.

4.5.1 Publishing CVE Records

4.5.1.1 CNAs MUST provide CVE Record content that meets the requirements listed in section 5.

4.5.1.2 CNAs MUST publish CVE Records to the CVE List through the process designated by the CVE Program.

4.5.1.3 CNAs SHOULD publish a CVE Record to the CVE List within 24 hours of Publicly Disclosing a CVE ID assigned by the CNA. CNAs MAY publish or update CVE Records as part of the CNA’s processes to manage Vulnerability advisories or other public information that references the CVE ID.

4.5.1.4 CNAs MUST publish a CVE Record to the CVE List within 72 hours of Publicly Disclosing a CVE ID assigned by the CNA. If the CNA does not publish within 72 hours, then the CNA’s Root MAY direct the appropriate CNA-LR to publish a CVE Record for the assigned CVE ID. Ownership of the CVE Record MAY be transferred. See also 4.2.1.2.

4.5.1.5 In exigent circumstances, for Publicly Disclosed Vulnerabilities, when a CNA with appropriate scope has not published a CVE Record, an appropriate TL-Root MAY direct an appropriate CNA-LR to publish a CVE Record. Ownership of the CVE Record SHOULD be transferred.

4.5.1.6 CNAs SHOULD publish CVE Records within 72 hours of becoming aware that a CVE ID assigned by the CNA has been Publicly Disclosed by a party other than the CNA.

4.5.1.7 The Secretariat MAY publicly identify the CNA who reserved the CVE ID 24 hours after a CVE ID has been Publicly Disclosed. Otherwise, the Secretariat SHOULD NOT publicly identify the CNA until the CVE Record has been published.

4.5.2 Publishing Vulnerability Information

4.5.2.1 CNA SHOULD publish Vulnerability advisories or other information about Vulnerabilities for which the CNA has assigned CVE IDs and published CVE Records. Such information SHOULD meet the public references requirements in 5.3 and MAY be used as a public reference (see 5.3.1.1).

4.5.2.2 Supplier CNAs MUST have at least one distribution point, such as a web site, where the CNA publishes Vulnerability advisories or other information about Vulnerabilities for which the CNA has assigned CVE IDs and published CVE Records. This Vulnerability information SHOULD reference appropriate CVE IDs.

4.5.2.3 The Vulnerability information described in 4.5.2.1 MUST generally support and MUST NOT contradict information published by the CNA in corresponding CVE Records.

4.5.2.4 The distribution point and Vulnerability information MUST be publicly accessible, MUST NOT require registration or login, and MUST NOT impose terms of use that restrict general-purpose use of the information or contradict the CVE Program Terms of Use.

4.5.2.5 CNAs MAY provide additional information under more restrictive terms of use or access controls.

4.5.2.6 CNAs SHOULD consider the long-term availability of Vulnerability information, especially when used as public references in CVE Records. CNAs SHOULD maintain URL availability through techniques such as URL redirects or by submitting references to archival services such as the Internet Archive or other mechanisms determined by the CVE Program.

4.5.2.7 Supplier CNAs MUST inform the Secretariat about the CNA's distribution point(s). This information will be published in the List of Partners.

4.5.3 Changes to CVE Records

As new information becomes available, CNAs can make changes to the content of published CVE Records and the number of CVE IDs assigned to one or more Vulnerabilities.

4.5.3.1 CNAs SHOULD update published CVE Records when information material to the Record changes, for example, when a Fix becomes available.

4.5.3.2 CNAs SHOULD update materially incorrect information in published or rejected CVE Records.

4.5.3.3 CNAs MAY update published CVE Records and SHOULD consider the cost of updates, the age of the CVE Record, and the value of the new information.

4.5.3.4 In exigent circumstances, when the CNA has not updated the CVE Record with a critical change or correction, and at the discretion of an appropriate TL-Root, the TL-Root MAY request that the Secretariat update the CVE Record.

4.5.3.5 CNAs MUST reject unused or unpublished CVE IDs.

4.5.3.6 CNAs MAY reject published CVE Records. Common reasons to do so include determining that no Vulnerability exists, using an incorrect CVE ID, duplicate assignment, or the combination or merging of multiple CVE IDs.

4.5.3.7 When deciding to reject a published CVE Record, CNAs MUST use the formats and mechanisms specified by the CVE Program and MUST provide an explanation.

4.5.3.8 CNAs MAY combine or merge CVE ID assignments. CNAs MUST reject published CVE IDs and CVE Records that become redundant after the change. When deciding which CVE IDs and CVE Records to reject, CNAs SHOULD consider factors such as the time of publication and the extent of public use and awareness.

4.5.3.9 CNAs MAY separate or split CVE ID assignments, assigning new CVE IDs and publishing corresponding CVE Records as necessary.

4.5.3.10 When marking a published CVE Record as disputed, CNAs and the Secretariat MUST use the formats and mechanisms specified by the CVE Program, MUST use the "disputed" tag, and MUST provide an explanation in the CVE Record. See also 5.1.11.

4.5.3.11 CVE Program members MUST indicate “disputed” status and present the explanation when rendering and displaying CVE Record data.

4.5.4 CVE ID Ownership and Transfers

4.5.4.1 The ownership of a CVE ID and the corresponding CVE Record SHOULD NOT be transferred except in specific circumstances, primarily related to issues with scope or delays in assignment or publication, as determined by the appropriate Root. For example, if a CNA assigns a CVE ID and publishes a corresponding CVE Record, and at the time of assignment a different CNA had more appropriate scope, then the appropriate Root SHOULD transfer ownership of the CVE ID to the CNA with more appropriate scope.

4.5.5 CVE Record Formatting and Interfaces

4.5.5.1 CNAs MUST submit CVE Records in the formats and through the mechanisms specified by the CVE Program.

4.5.5.2 The CVE Program MUST provide a non-production environment and reasonable time periods during which CNAs can test changes to formats and mechanisms.

4.5.5.3 CNAs MUST handle changes to formats and mechanisms within test periods.

4.6 Dispute Resolution

It is expected that there will be disagreement about Vulnerability determination, CVE ID assignment decisions, and the content of CVE Records.

4.6.1 CNAs or other parties who disagree with a Vulnerability determination, CVE ID assignment, or the content of a CVE Record MAY dispute the determination, assignment, or content.

4.6.2 CNAs SHOULD work with relevant parties to attempt to resolve disputes before initiating the CVE Program Policy and Procedure for Disputing a CVE Record.

4.6.3 Disputes MUST follow the process described in CVE Program Policy and Procedure for Disputing a CVE Record.

5 CVE Record Content

This section specifies what information is in a CVE Record.

5.1 Required CVE Record Content

This section defines the minimum content required in a CVE Record. A CVE Record:

5.1.1 SHOULD contain sufficient information to uniquely identify the Vulnerability and distinguish it from similar Vulnerabilities.

5.1.2 SHOULD identify the vulnerable Products, versions, dates, components, sub-components, features, modules, APIs, functions, function calls, commands, utilities, or programs, to the degree necessary to uniquely identify the Vulnerability.

5.1.3 MUST identify at least one affected Product using information such as Supplier and Product names, versions, and dates.

5.1.4 MUST identify at least one Product as “affected” or “unknown” (with the possibility of being affected).

5.1.5 SHOULD identify Fixed versions of Products.

5.1.6 SHOULD resolve “Unknown” status (to “affected” or “unaffected”) within a reasonable timeframe. A permanent “Unknown” status MAY be appropriate if, for example, a Product is suspected of being affected but has not been investigated.

5.1.7 MUST identify the type of Vulnerability. The CVE record SHOULD use the Common Weakness Enumeration (CWE) to classify the type or cause of the Vulnerability. A CVE Record MAY contain multiple types or causes of the Vulnerability.

5.1.8 MUST NOT only contain Products with “unaffected” status. This would not be a Vulnerability.

5.1.9 MUST contain a prose description (see 5.2).

5.1.10 MUST contain at least one public reference (see 5.3).

5.1.11 MUST include the appropriate and approved CNA tag(s), if applicable. CVE Program members SHOULD present the information provided by tags, including relevant explanations, when rendering and displaying CVE Record data.

5.1.11.1 MUST use the "exclusively-hosted-service" tag when all known Products listed in the CVE Record exist only as fully hosted services. If the Vulnerability affects both hosted services and on-premises Products, then this tag MUST NOT be used.

5.1.12 MUST meet any requirements set by any approved formats or submission mechanisms, for example, the CVE Record Format and the Record Submission and Upload Service (RSUS). Such requirements will be integrated into this document on a periodic basis.

5.1.13 MAY contain optional elements supported by the CVE Record Format.

5.2 Description

Through automation efforts such as the CVE Record Format and CVE Services, the content of the prose description in a CVE record is becoming less important. The prose description is still useful in providing sufficient information to uniquely identify the Vulnerability and distinguish it from similar Vulnerabilities. The description:

5.2.1 MUST summarize the Vulnerability, using, for example, information from 5.1.1 through 5.1.7.

5.2.2 MUST include any information required by 5.1 that is not provided by a more specific part of the CVE Record Format.

5.2.3 MUST NOT contradict information provided elsewhere in the CVE Record.

5.2.4 MUST NOT credit people, organizations, or tools. CNAs MAY credit or acknowledge people, organizations, or tools in their own Vulnerability advisories or other information about Vulnerabilities or using the optional “credits” or “source” elements of the CVE Record Format.

5.2.5 MUST include one description in English and MAY include descriptions in other languages.

5.2.6 MUST NOT contain information that is not relevant to identifying and describing the Vulnerability, for example, inappropriate language or advertising.

5.2.7 SHOULD NOT only describe one CVE Record as being different than another CVE Record. Different CVE IDs MUST identify different Vulnerabilities.

5.2.8 MAY follow examples found in Key Details Phrasing.

5.2.9 MAY duplicate information provided elsewhere in the CVE Record.

5.2.10 MAY be automatically generated from elements of the CVE Record.

5.2.11 SHOULD NOT contain Vulnerability identifiers that are not CVE IDs unless the Vulnerability identifiers are necessary to specifically describe or identify the Vulnerability. CNAs MAY include Vulnerability IDs using public references or other elements of the CVE Record Format.

5.3 Public References

Public references support the information contained in CVE Records.

5.3.1 CNAs MUST ensure that a public reference exists on the internet before or concurrently with the publication of the corresponding CVE Record. A CVE Record MUST NOT be the first Public Disclosure of a Vulnerability.

5.3.1.1 If a CNA publishes advisories or other information about Vulnerabilities as described in 4.5.2, that information SHOULD also meet the public references requirements in 5.3 and MAY be used as a public reference (see 4.5.2.1).

5.3.1.2 If multiple public references exist, CNAs MUST include the most freely available public reference in the CVE Record.

5.3.2 CNAs SHOULD consider the long-term availability of public references, for example, by submitting references to archival services such as the Internet Archive or other mechanisms determined by the CVE Program.

5.3.3 A CVE Record MUST have at least one public reference that:

5.3.3.1 SHOULD NOT require registration or login, and

5.3.3.2 SHOULD NOT impose terms of use or service that restrict general-purpose use of the information or contradict the CVE Program Terms of Use, and

5.3.3.3 MUST contain information about the specific Vulnerability, and

5.3.3.4 MUST provide the minimum information required to support the content of the CVE Record (see 5.1).

5.4 Example or Test CVE IDs

5.4.1 For example, documentation, and testing purposes, CVE Program participants SHOULD use CVE IDs with the prefix 'CVE-1900-' that otherwise conform to the current CVE ID specification.

5.4.2 CVE Program participants MUST treat CVE IDs and CVE Records using the 'CVE-1900-' prefix as test or example information and MUST NOT treat them as correct, live, or production information. The CVE Services do not support CVE IDs with this prefix.