# CNA Processes

This document describes the common set of processes that a CVE Numbering Authority (CNA) should execute in their role as a CNA. Questions about these processes or assistance with integrating these processes into a CNA’s internal operations can be directed to the [CVE Request Form](https://cveform.mitre.org/) or to [cve@mitre.org](mailto:cve@mitre.org). Note, these processes assume the CNA reports up directly to the Primary CNA. If the CNA reports up to a Root CNA, the Root CNA may have its own set of processes that must be followed.

## General Workflow

CNAs follow similar workflows when performing CNA tasks as part of their larger vulnerability management or disclosure processes. CNAs must request and manage their CVE ID block, assign CVE IDs, have the CVE ID entries in the CVE List be populated, and update those entries as necessary. The following sections describe this workflow in more detail.

## Requesting a CVE ID Block

CNAs are allocated one or more blocks of CVE IDs each year from which they may assign CVE IDs to vulnerabilities in their scope. A block of CVE IDs will be a contiguous range of CVE IDs. CVE IDs that are allocated to a CNA are marked as “RESERVED” in the CVE List until the CVE entry has been [populated](#_Populating_CVE_Entries). The block of CVE IDs will come from a CNA’s parent CNA, so CNAs that report to the Primary CNA will request their blocks from the Primary. Those with a Root CNA above them will request their blocks of IDs from their Root.

CNAs must request a new block of CVE IDs each calendar year. This request can be made at any time, though it is best practice for most CNAs request a block in the last quarter of the current year.

CNAs can request a block of any size (the CVE Request Form limits the maximum request size to 999, but a CNA may ask for more), though the size should be tied to the number of CVE IDs that the CNA expects to assign plus a reasonable extra amount to account for unexpected assignments. For example, one CNA may expect to assign over 800 CVE IDs each year, so they will request a block of 1000 CVE IDs each year. Another CNA may expect to assign only 10 CVE IDs each year, so they will request 15 CVE IDs each year. This prediction can vary and depend on past experience, plans for changes to product lines, or changes to how vulnerabilities are managed by the CNA.

There is no harm in predicting incorrectly. If a CNA requests fewer CVE IDs than they need in a year, they can easily request another block. If a CNA requests more CVE IDs than they need, the excess CVE IDs will expire at the end of the year. See [CVE ID Expiration](#_CVE_ID_Expiration) below.

Note, CVE ID block requests can be denied for a number of reasons. For example, if a CNA repeatedly violates the CNA Rules, requests for new CVE IDs may be denied or delayed until the CNA remedies the problematic issues. The Primary CNA will communicate closely with a CNA to remediate problems as quickly as possible.

To request a block of CVE IDs from the Primary CNA, visit the [CVE Request form](https://cveform.mitre.org/) and select the “Request a block of IDs (CNAs only)” request type. Complete and submit the request, and you should receive an email message including your CVE ID block information within two business days. If your request needs to be rushed (because you have run out of CVE IDs and need to make an assignment as soon as possible, for example), submit your request as above and email [cve@mitre.org](mailto:cve@mitre.org) requesting that your block request be expedited. (Note, Root CNAs may have their own processes for fulfilling CVE ID block requests.)

## CVE ID Expiration

All CVE IDs include a year as part of their label. This year indicates what year the CVE ID was assigned. Each year, a new block of CVE IDs is given to CNAs upon request, and those new CVE IDs should be assigned to a vulnerability in the new year. (For example, CVE-2017-nnnn should be assigned in the calendar year 2017, whereas CVE-2018-nnnn should be assigned in the calendar year 2018.)

Unassigned CVE IDs for a given year expire at the end of that year. At the beginning of each calendar year, CNAs must notify their parent CNA as to which CVE IDs have not been assigned from the previous year. Those notifications will be escalated to the Primary CNA, who will mark any CVE IDs that are expired as REJECTED with a description stating they were unused.

Note, the year a CVE ID was assigned does not have to match the year it was published. For example, a CNA could assign a CVE ID in 2017 and not publicly reference that CVE ID until 2018, when it would in turn be populated in the CVE List.

## Assigning CVE IDs

Assigning CVE IDs to vulnerabilities is the primary role of a CNA. CVE ID assignment includes the process known as CVE Counting, described in Appendix C of the CNA Rules, and the collection and formatting of information that describes the vulnerability assigned to the CVE ID.

In general, the process of assigning CVE IDs is as follows. First, a requester triggers the process by sending vulnerability information and requesting a CVE ID. This request may come from a stakeholder internal to the CNA or from an external source. The CNA must then acknowledge receipt of the request per the CNA’s established communication processes and adhering to their disclosure and embargo policies.

The CNA must then perform Counting on the request to determine the number of CVE IDs to assign. The CNA should then notify the requester of the CVE ID assignment and any other information relevant to the assignment depending on their disclosure and embargo policies.

When the CNA is prepared to publicly disclose the vulnerability details related CVE ID assignments, the CNA should request that the CVE Entries for the CVE IDs in question be changed from RESERVED to populated. It is important that a CNA follow-through on this next step.

## Populating CVE Entries in the CVE List

The process of taking a description, references, and other related data for a CVE entry and publishing that information in the CVE List is referred to as “populating” a CVE entry. Though a CVE ID may be assigned to a vulnerability and be referenced publicly, until the CVE entry has been populated properly, the CVE entry will show as “RESERVED” in the CVE List.

As a general guideline, once a CNA has used a CVE ID publicly, such as in a public advisory, the CNA has one business day to request the population of the associated CVE entry. The CNA must create a population request, format it correctly, and submit that request to their Root CNA or the Primary CNA, depending on their Root CNA’s communication rules. See the CNA Rules for the current minimum standard for CVE ID population.

If the request is made through a Root CNA, the Root CNA should relay that request up to the Primary CNA within one business day. The Primary CNA will populate the CVE entry and publish it as part of the CVE List.

The permitted formats for CVE entry population requests are described in the [CNA Rules document](http://cve.mitre.org/cve/cna/CNA_Rules_v1.1.pdf). The preferred format is the JSON submission format found [here](https://github.com/CVEProject/automation-working-group/tree/master/cve_json_schema). Submissions can also be made through the [CVE Request Web Form](https://cveform.mitre.org/), and the submissions should be formatted in JSON or the flat-file format described in Appendix B of the CNA Rules.

## Updating CVE Entries

CVE entries may be updated for a number of reasons; e.g., duplicate entries, incorrect counting, disputes, reference updates, and description updates. Throughout this process, we are careful to preserve as much information about the actions taken as possible. Therefore, even when rejecting a CVE ID, we still include that CVE ID in the CVE List with some information about the cause of its rejection.

In general, the process for updating a CVE entry is the following. First, a CNA will receive the request, whether that be from an internal stakeholder or an external consumer. The CNA who received the request will determine if the CVE entry in question is under the scope of a different CNA. If yes, the latter CNA would be notified.

Once the correct CNA has been given the request, that CNA will validate the request. If the request requires an update, the CNA will ask the Primary CNA to update the CVE entry by

* Updating the CVE ID entry’s references or description;
* Rejecting the CVE ID outright;
* Merging two CVE entries;
* Splitting a CVE entry; or
* Disputing a CVE entry.

A request to update a CVE entry can be made through the CVE Request form though the “Request an update to an existing CVE Entry” request type or through whatever other process a CNA uses to send information to their parent CNA. New information or corrected information related to the CVE entry can be included, and specific types of changes can be requested, including rejection, merging, splitting, or disputing.

## Rejecting a CVE ID

There are many reasons why a CVE ID may be rejected, such as further research determining the issue is not a vulnerability, a typo in an advisory causes the wrong CVE ID to be used, or the researcher decides to keep the vulnerability private. In these and other instances, the description for the CVE entry is updated to reflect that the CVE ID has been REJECTED and provides the reason for the rejection. Rejecting a CVE ID is often part of another change or set of changes being made, as shown below.

## Merging Two CVE Entries

Occasionally, multiple issues that are assigned to different CVE IDs are found to actually be the same issue. In this case, the issues should be consolidated into one CVE ID. This consolidation process is known as “merging” the CVE entries. When this happens, associate the issues with the CVE ID that meets the following criteria. (Note, here only two CVE entries are merged, but this process is the same for any number of duplicate CVE entries.)

Using public sources, we first determine which CVE ID should be associated with the issue. We then merge the information into the chosen CVE ID. Finally, we update the CVE ID that was not chosen with “REJECT” status and include a new description that points to the chosen CVE ID directing consumers to use the chosen CVE ID for the vulnerability instead.

To determine which CVE ID should be associated with the issue, we use the following decision process:

1. If one CVE ID is more commonly referenced than the other, we choose the more commonly used. This can be roughly gauged by searching for all affected CVE IDs on a set of search engines and compare the results between the two.
2. If the CVE IDs are referenced with the same frequency, we choose the CVE ID used by the most authoritative source. The most authoritative source can be roughly prioritized as vendor, coordinator, then researcher.
3. If the CVE IDs have the same level of authority and are referenced with the same frequency, we choose the CVE ID that has been public (based on when it was populated in the CVE List) for the longest period of time.
4. If there is still a doubt as to which CVE ID should be associated with the issue, we choose the identifier with the smallest numeric portion.

Note that the process described above is reserved for cases where the CVE IDs have clearly been assigned to the same vulnerability. If there is insufficient information to decide, the description of the CVE entries may be changed to indicate that they may be the same. For example, a NOTE sentence such as "This may be the same as <the-other-CVE-ID>" or "This may overlap <the- other-CVE-ID>" may be used.

## Splitting a CVE Entry

Occasionally, multiple issues all associated with the same CVE ID are found to actually be separate issues that are unique vulnerabilities that should each by assigned a CVE ID. When this happens, we will associate the original CVE ID with the issue that is least likely to conflict with the general public's "perception" of what the original CVE ID refers to. The rest will each receive a new CVE ID. This is referred to as “splitting” a CVE entry.

Using public sources, we attempt to determine:

1. If the CVE ID is associated with one particular issue more often than others. If so, we associate that issue with the ORIGINAL ID and assign new CVE IDs to the others; or
2. If the association is the same for each issue, then we pick the issue with the most severe risk and associate that issue with the original CVE ID and assign new CVE IDs to the others; or
3. If the risks are the same and have the same association for each issue, then we pick the issue with the broadest range of affected versions and associate that issue with the original CVE, assigning new CVE IDs to the others; or
4. If all previously-mentioned factors appear to be equal, look at the raw disclosure, find the issue that is described first, and associate that issue with the original CVE ID.

## Disputing a CVE Entry

Not everyone shares the same definition of a vulnerability. One person’s vulnerability is another person’s security hardening opportunity or another person’s intended functionality. When an authoritative source disputes the validity of the vulnerability, “\*\* DISPUTED \*\*” is added to the beginning of the description, and a short NOTE is added to the end explaining why the vulnerability is disputed. Ideally, the disputing party provides a link that can be added to the CVE as a reference and a quote that can be used as the explanation in the NOTE. However, neither are required.

Note that marking a CVE entry as disputed is different from rejecting a CVE entry. Rejections are made because the issue is clearly not a vulnerability (it fails CNT2 in the Counting Rules), the vulnerability is not made public (it fails INC2 in the Counting Rules), the product isn't customer controlled (it fails INC3 in the Counting Rules), or the product is not generally available (it fails INC4 in the Counting Rules). Entries are disputed when there are differing opinions about it being a vulnerability or regarding the specific details of the vulnerability itself. The more binary cases of INC2, INC3, and INC4 are not things that can be disputed, per se. They either are or are not true.

## Partial Duplicate Issue

There are cases where two existing CVE IDs overlap in what software or hardware is affected by the same vulnerabilities. An example of this would be if CVE-2017-nnnn1 references Product1 versions 1.0, 2.0, and 3.0 and CVE-2017-nnnn2 is assigned to the same vulnerability and references Product1 versions 3.0, 4.0, and 5.0. In this situation, use the following process, which uses a similar process to a regular merge process.

1. We prefer the most commonly referenced CVE ID. This is roughly gauged by searching for all affected CVE IDs on a search engine and comparing results. In our example above, CVE-2017-nnnn1 is used more often than CVE-2017-nnnn2. Therefore, CVE-2017-nnnn1 would reference versions 1.0, 2.0, and 3.0, and CVE-2017-nnnn2 would be changed to only reference versions 4.0 and 5.0. In both CVE entries, a note should be added to the effect "This CVE entry is related to [the other]."
2. If the usage numbers of CVE IDs are about the same, then we choose the CVE ID used by the most authoritative source. The most authoritative source is roughly prioritized as vendor, coordinator, then researcher. Again, if CVE-2017-nnnn1 is used by the most authoritative source, CVE-2017-nnnn1 would reference versions 1.0, 2.0, and 3.0, and CVE-2017-nnnn2 would be changed to only reference versions 4.0 and 5.0. In both CVE entries, a note should be added to the effect "This CVE entry is related to [the other]."
3. If the CVE IDs have the same level of authority, then we choose the identifier that has been public for the longest period of time. Again, if CVE- 2017-nnnn1 has been public for the longest period, CVE-2017-nnnn1 would reference versions 1.0, 2.0, and 3.0, and CVE-2017-nnnn2 would be changed to only reference versions 4.0 and 5.0. In both CVE entries, a note should be added to the effect "This CVE entry is related to [the other]."
4. If the CVE IDs have been public for the same amount of time, then we choose the identifier with the smallest numeric portion. Since CVE-2017-nnnn1 uses a smaller numeric portion, CVE-2017-nnnn1 would reference versions 1.0, 2.0, and 3.0, and CVE-2017-nnnn2 would be changed to only reference versions 4.0 and 5.0. In both CVE entries, a note should be added to the effect "This CVE entry is related to [the other]."
5. If there are any disputes after this, we choose the CVE ID that was populated earliest in the CVE List. Assuming CVE-2017-nnnn1 was populated earliest, CVE-2017-nnnn1 would reference versions 1.0, 2.0, and 3.0, and CVE-2017-nnnn2 would be changed to only reference versions 4.0 and 5.0. In both CVE entries, a note should be added to the effect "This CVE entry is related to [the other]."

Note that the process described above is reserved for cases where the CVE IDs have clearly been assigned to the same vulnerability. If there is insufficient information to decide, the description of the CVE entries may be changed to indicate that they may be the same. For example, a NOTE sentence such as "This may be the same as..." or "This may overlap..." may be used.

## Working with Vulnerabilities Found in an Upstream Developer’s Code

If a CVE ID is being assigned to a vulnerability, the CNA MUST make a reasonable effort to notify the maintainer of the code in which that vulnerability exists. (If the CNA is assigning for a vulnerability in their own product or codebase, this is inherently done.) For example, if an operating system vendor discovers a vulnerability in a printing library they distribute, in addition to assigning the CVE ID to the vulnerability, they should attempt to contact the upstream developer. This will help avoid duplicate CVE ID assignments as well as ensure others that are affected by the vulnerability will be made aware of it.

## Escalating

The structure of the CNA program gives consumers and participants a natural path to follow when problems or issues must be escalated or communicated downstream to the responsible party. Refer to \*\*\*CVE ID Issue Resolution\*\*\* for a description of situations where escalation or dissemination may occur.

Typically, a problem or issue with a CVE ID should be addressed by the CNA who assigned the CVE ID. If that CNA is unresponsive or if that CNA has reached an impasse with whoever has brought the problem or issue to them, the problem or issue can be escalated.

The requestor can escalate to the appropriate Root CNA or the Primary CNA. The Root/Primary CNA will communicate with both the requester and the CNA to understand the details of the situation and the reasoning behind the CNA’s decision. The Root/Primary will then determine what action is appropriate and inform all parties of its decision.

If an issue is escalated to the Primary CNA, the Primary CNA makes the final decision regarding the issue. In these cases, it is important that the CNA provide as much information as possible about the issue when working with their Root CNA or the Primary CNA. If information about the issue is missing or left unstated, the final decision made by the Root CNA or Primary CNA could be negatively affected.

## Terms and Definitions

|  |  |
| --- | --- |
| Term | Definition |
| CVE List | A collection of common names (CVE IDs) for publicly known cybersecurity vulnerabilities. |
| CVE ID Block | A set of sequential CVE IDs given to a CNA for later assignment to vulnerabilities. |
| CVE Entry | An item in the CVE List. CVE entries contain the CVE ID, a description of the vulnerability, and references to public disclosure sources. |
| Populate | The act of filling in the details for a previously reserved CVE ID into the CVE List. |
| Reserved CVE ID | A CVE ID that has been given to a CNA for assignment and has not had the vulnerabilities details populated in the CVE List. |