# **CVE ID Request Guidelines**

This document provides information on how to determine if a vulnerability should be assigned a CVE ID, recommended steps to coordinate the disclosure of a vulnerability, where and how to request a CVE ID for a new vulnerability, and how CVE IDs are shared in public disclosures.

# Determine if a Vulnerability Needs a CVE ID

CVE IDs are typically requested by vulnerability discoverers or software maintainers. However, any person may request an ID for a vulnerability that is not yet present in the CVE List. The following steps should be taken to determine if a CVE ID should be requested:

1. Determine whether the identified problem meets the CVE program’s definition of a vulnerability.
	* A vulnerability in the context of the CVE program is a weakness in the computational logic (e.g., code) found in software and some hardware components (e.g., firmware) that, when exploited, results in a negative impact to confidentiality, integrity, OR availability. Mitigation of the vulnerabilities in this context typically involves coding changes, but could also include specification changes or even specification deprecations (e.g., removal of affected protocols or functionality in their entirety).
	* In general, a CVE ID is for customer-controlled software and cannot be assigned for a vulnerability affecting a single web site or online service.
2. Ensure that the identified vulnerability will be publicly announced.
	* CVE IDs are assigned only to vulnerabilities that are public or are going to be publicly announced.
3. Ensure that a CVE ID does not already exist for the vulnerability.
* Perform a keyword search on the [CVE List](http://cve.mitre.org/cve/cve.html).
* Perform a general web search.
* Search resources that are specific to the vendor or software type, such as vendor security advisories or security mailing lists.

# Coordinate Vulnerability Disclosure with the Software Maintainer

If a CVE ID is needed, coordinated vulnerability disclosure with the software maintainer is highly recommended. Coordinated disclosure is a risk-management process for cases in which a vulnerability discoverer is not the primary maintainer of the affected software[[1]](#footnote-1). The core principle of coordinated disclosure is that the discoverer and the software maintainer work together to provide public disclosure after a fix to the vulnerability is available. For example, when an independent researcher discovers a vulnerability in a product maintained by a vendor or when a software user discovers a vulnerability in software maintained by an Open Source project (often called an "upstream" project).

Instances where coordinated disclosure is NOT necessary, or possible, include:

 1. The vulnerability was discovered by the software maintainer or vendor.

 2. The vulnerability was already reported to the software maintainer or vendor by a party (such as a customer) who does not wish to be involved in the vulnerability-management process.

 3. The vulnerability has already been disclosed in a public forum.

If a discoverer’s situation is covered by any of these cases, then this coordination section does not apply. If the situation does not fall into the cases above, then a coordinated disclosure is highly recommended to provide the maintainer with the opportunity to fix the vulnerability before a public announcement.

Key points to help a discoverer coordinate a vulnerability:

* Review the scope of CVE Numbering Authorities (CNAs)[[2]](#footnote-2) on CVE website
	+ If a CNA is identified skip to section 3 “Requests to a Vendor CNA”.
* Find a vendor contact
	+ To find a contact method for a non-CNA, use a public contact list or consult the vendor’s web site for contact information. At present, the best public contact list is the HackerOne.com directory.
		- Major software producers often have a specific contact method for vulnerability reports.
		- Minor software producers sometimes have a general contact method listed on their web site.
		- Vendors may use bug bounty programs to incentivize researchers to provide information on vulnerabilities and facilitate communication. Bug bounty programs can be run by a vendor, run by a third-party associated with the vendor, or a third-party that has no association with the vendor.
* Determine confidence in vulnerability identification and uniqueness
	+ In most cases, CVE IDs should be requested after feedback is received from the software maintainer validating the vulnerability.
	+ To receive a CVE ID before obtaining validation from the software maintainer, the discoverer needs a high level of confidence that the vulnerability is legitimate.
* Include the CVE ID in communications
	+ If a CVE ID already exists, include it in communications with the software maintainer or vendor to reduce the likelihood of a duplicate CVE entry.
* Set response expectations
	+ Determine a reasonable amount of time for a software maintainer or vendor to respond to communications. Appendix A provides examples of a structured vulnerability-contact process.

If there **is** a response, then the discoverer should coordinate with the software maintainer to determine:

1. Which party (discoverer or software maintainer) will request the CVE ID?
2. Does the discoverer wish to test the patch before the public release of the patch?
3. On what specific date will public disclosure occur?
4. How much detail should be included in the public disclosure?

If there is NO response to an initial contact, additional options include:

* Attempt to enlist a third-party coordinator by using <https://vulcoord.cert.org/VulReport/> or a similar resource within a discoverer’s country. Third-party coordinators assist discoverers that are having trouble reaching a software maintainer with coordinating and disclosing a vulnerability within the Coordinator’s scope. Third-party coordinators do not assign CVE IDs for vulnerabilities in products covered by another CNA. Note that the MITRE CVE Team is NOT a vulnerability coordinator.
* Make multiple contact attempts to the software maintainer and wait longer for a response.

If there is still no response, then the discoverer should use their judgment about the best way to balance the risks of uncoordinated disclosure with the risks of no disclosure at all. If the discoverer decides to make a public disclosure they should use the MITRE [CVE Request web form](https://cveform.mitre.org/) to notify the MITRE CVE Team of the disclosure's URL (e.g., a URL for an archive of a post to a security mailing list or a URL of a blog post). Further, if the vendor is not responsive, the discoverer should include a detailed timeline showing the dates and attempted contacts with the vendor and/or third-party coordination bodies to demonstrate that they made a reasonable effort to coordinate.

# Requests to a Vendor CNA

CNAs are organizations authorized to work with researchers, vulnerability discoverers or reporters, and information technology vendors to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed upon scope. Often, the CNA’s distinct, agreed upon scope, is all products from a single vendor. In some instances, a CNA’s scope can include multiple vendors. For example, the scope of the HackerOne CNA includes dozens of vendors[[3]](#footnote-3). The list of CNAs can be found on the [CVE](http://cve.mitre.org/cve/request_id.html#cna_coverage.html) website.

CNAs have the flexibility to administer their own vulnerability management process. Once a vulnerability is confirmed, the CNA assigns a CVE ID within their established timeframes. Any questions on CVE ID assignment timeframes should be directed to the responsible CNA. Once the CVE ID is assigned and the vulnerability made public, the CNA provides MITRE with the CVE entry details. MITRE is responsible for publishing the CVE List and for addressing any issues in the operation of the CNA program. MITRE can be contacted as shown on the [CVE](https://cve.mitre.org/about/contactus.html) website.

# Requests to MITRE (Primary CNA)

If the organization responsible for assigning the CVE ID is MITRE, or there is no other organization responsible for assigning a CVE ID, discoverers should complete MITRE’s [CVE Request web form](https://cveform.mitre.org/) to request a CVE ID. After the CVE Request is submitted, the “discoverer” becomes the “requester”.

## Information to Provide in the Request to MITRE

The "*Request a CVE ID*" selection on MITRE's CVE Request web form can be used in the following cases:

1. Private CVE ID Reservation: The requester wishes to obtain a CVE ID but requires that the vulnerability information remain private until further notice. This is called a private CVE ID reservation where the information has an embargo that ends upon a future communication from the requester.
2. Public CVE ID Assignment: The requester wishes to obtain a CVE ID and wishes to have the vulnerability information made public in the CVE List immediately. This is called a public CVE ID assignment.

For a Private CVE ID Reservation, a "*Request a CVE ID*" form requires, at a minimum, the following information:

* The type of request
* The e-mail address of the requester
* The number of IDs being requested
* The type of vulnerability for each CVE ID requested
* The affected vendor for each vulnerability
* The affected product and version(s) for each vulnerability

VERY IMPORTANT: If your form submission includes a public reference URL, it may be interpreted as a Public CVE ID Assignment. Please be sure to use the Additional Information field to clarify all cases in which a reference URL is included for a Private CVE ID Reservation. For example, if the URL itself is supposed to be secret, even though the URL content can be read by any web-site visitor, such as a gist.github.com URL. The CVE Team carefully considers the Additional Information field before placing any vulnerability information into the public CVE List.

In addition to the required information identified above, a Public CVE ID Assignment also requests a "*Suggested description of the vulnerability for use in the CVE*" entry and at least one publicly-accessible URL reference. Providing a suggested CVE description helps ensure that the vulnerability is added to the CVE List as quickly as possible.

In addition to the minimum required information, optional information can be included to provide additional detail for the CVE ID request. This optional information is valuable in creating the CVE entry and to downstream consumers looking to understand vulnerabilities in the CVE List, generate CVSS scores, and differentiate between vulnerabilities. Information provided in the CVE entry should be consistent with public references and should not include any private or non-public information.

## Confirmation of request to MITRE

Upon completion of the CVE Request web form, the requester receives a confirmation email with a reference number. To communicate with MITRE about this request, requesters should reply to the confirmation email without changing the subject line, as it contains the reference number associated with the request. Requesters should check their spam folder if a confirmation email is not received. If an email was not received, contact the MTIRE CVE team at cve@mitre.org.

## Follow-up information requests from MITRE

If MITRE requires any additional clarification, they will contact the requester via email citing the reference number for the submitted CVE Request.

## Receive a CVE ID (or rationale if not assigned)

Once there is enough information to confirm that a new vulnerability exists,

the MITRE CVE Team will reply to the requester with a CVE ID. The reply will include the entered web form information. At this stage, the CVE ID is considered "reserved" and remains reserved until the vulnerability is made public (see step 7). The MITRE CVE Team may edit the CVE entry if an adjustment to the number of CVE IDs assigned is required or if additional clarification is needed.

If the CVE Team determines that the submission was misdirected to MITRE, is inconsistent with the definition of a vulnerability, or is or is determined to be a duplicate, a CVE ID request may be rejected. In this case, the requester will receive an email response from the MITRE CVE Team notifying them of the decision. This email will contain all the entered form information, in case the requester requires the information for resending to a different CNA or to a different publication outlet, such as a vulnerability website, to obtain community input on the vulnerability.

# Sharing the CVE ID with others.

Once a CVE ID is assigned, the requestor should provide it to all parties involved in the coordinated disclosure process. This makes it easier to share information about the vulnerability and reduces the risk that different parties may assign different CVE IDs to the same vulnerability.

# Information to Include in a Vulnerability Announcement.

When publishing a vulnerability with an assigned CVE ID, the CVE ID should be included in the announcement. Announcements containing multiple CVE IDs should delineate which CVE ID is associated with which vulnerability.

The following information may be contained in the vulnerability announcement:

* The Common Vulnerabilities and Exposures (CVE) project has assigned the ID CVE-YYYY-NNNN to this issue. This is an entry on the [CVE List](http://cve.mitre.org/cve/index.html), which standardizes names for security problems.
* https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-YYYY-NNNN
* CVE ID: CVE-YYYY-NNNN

When announcing more than one CVE ID, associate each CVE ID with the assigned vulnerability, so that people can easily identify which CVE ID is related to each issue. For example:

* CVE-YYYY-NNNN - buffer overflow in product
* CVE-YYYY-MMMM - format string in product

# Notify the MITRE CVE Team of Publication

In the case of a Private CVE ID reservation that is later publicized, contact the MITRE CVE Team by either replying to the original email discussion or via the [CVE Request web form](https://cveform.mitre.org/). If you submit a new form, select "Notify CVE about a publication" and provide the following information:

* The CVE ID(s) assigned to the vulnerabilities being publicly announced.
* Links to the public forum(s) or advisories where the announcements can be found.

Until this information is provided to MITRE, the CVE entry is marked as “reserved” on the CVE web site. No description or details of the vulnerability is made available in the CVE repository until the vulnerability has been publicly announced elsewhere.

When notified of a publication, MITRE populates the CVE entry with the details provided by the requester. This information is available on the [CVE List](http://cve.mitre.org/cve/index.html).

The [U.S. National Vulnerability Database (NVD)](https://nvd.nist.gov/) will update their entries once the CVE ID entries have been made public.

**Appendix A: Documents on Disclosure Practices**

The following documents describe processes and provide guidelines for coordinated vulnerability disclosure practices.

1. "Guidelines for Security Vulnerability Reporting and Response," Organization for Internet Safety. Version 2.0, 01 September 2004.
<http://www.oisafety.org/> │ [http://www.symantec.com/security/OIS\_Guidelines%20for%20responsible%20disclosure.pdf](http://www.symantec.com/security/OIS_Guidelines%20for%20responsible%20disclosure.pdf%22%20%5Ct%20%22_blank%22%20%5Co%20%22Opens%20a%20PDF)
2. "Responsible Vulnerability Disclosure Process," IETF draft document, Christey/Wysopal. February 2002.
<http://tools.ietf.org/html/draft-christey-wysopal-vuln-disclosure-00>

**Appendix B: PGP Key**

You may encrypt any post-web form communications using PGP or GnuPG (gpg), with the following PGP key, which can be downloaded from various PGP key servers:

A PGP key is available for encrypted communications:

Key ID: 8B5618B6

Fingerprint: 3661 5122 7CF5 FC6B BCCC 7943 76FF 3305 8B56 18B6

Key size: 4096

Public key: Click to download

1. For more information on Vulnerability Coordination see <https://www.first.org/_assets/downloads/FIRST-Multiparty-Vulnerability-Coordination-draft.pdf>, [↑](#footnote-ref-1)
2. Refer to Section 3 “Requests to a Vendor CNA” for an overview of the role of CNAs. [↑](#footnote-ref-2)
3. These vendors are not directly listed but can be found through an [https://hackerone.com/directory](https://hackerone.com/directory%20) search. [↑](#footnote-ref-3)