# Researcher Reservation Guidelines

This document provides information on how to reserve a CVE ID(s) before publicizing a new vulnerability so that CVE IDs can be included in the initial public announcement of the vulnerability and can be used to track vulnerabilities.

Some important things to note:

- The CVE request process reduces the amount of overlap with the work of other entities by identifying which organization(s) should be contacted first.
- The CVE request process is designed to ensure all vulnerability information included in CVE is publicly available. This reduces the risk of accidental disclosure of such information. **Details provided in requests will not be released until those details have been made public.**
- If a requester does not use and share CVE IDs properly, MITRE and other CVE Numbering Authorities (CNAs) reserve the right to refuse assigning CVE IDs to that requester in the future. Steps 2, 10, 11, and 12 in the list below provide details on proper use and sharing of CVE IDs.

The basic process for reserving a CVE ID is as follows:

1. Determine if a CVE ID is needed and appropriate. If yes,
2. Contact a vendor whose product is affected to disclose a vulnerability (coordinated disclosure).
3. Determine whether the request should be made to a vendor CNA. If no,
4. Determine whether the request should be made to a third party coordinator CNA, or to a disclosure mailing list. If no,
5. Request a CVE ID from MITRE using the CVE Request web form.
6. Provide the required information in the request.
7. Receive a confirmation email with a reference number and save it for your records.
8. Provide follow-up information as needed.
9. Receive a CVE ID (or an explanation if a CVE ID was not provided)
10. Share the CVE ID with all parties.
11. Include the CVE ID in the announcement of the vulnerability.
12. Notify MITRE that the vulnerability has been made public using the CVE Request web form, and selecting “Notify CVE about a Publication.”

The CVE is then published by MITRE and will appear on the CVE List.

These steps are detailed in the sections below.

# 1 Determine if a CVE ID is needed and appropriate

CVE IDs are currently only assigned to vulnerabilities that are going to be publicly announced.

1. Determine whether the problem you identified is a vulnerability.

A vulnerability in the context of the CVE program is indicated by code that can be exploited, resulting in a negative impact to confidentiality, integrity, OR availability, and that requires a coding change, specification change, or specification deprecation to mitigate or address.”.

2. Ensure that the vulnerability for which you are seeking a CVE ID does not already have an assigned CVE ID by performing a keyword search on the CVE website.

# 2 Contact the affected product vendor directly

You should make a good faith effort to notify the affected vendor and work with them to ensure that a patch is available prior to publicly disclosing the vulnerability. Information is more accurate and complete when researchers and vendors work together. This practice also reduces the likelihood of a duplicate CVE ID being issued, which can happen when both a researcher and vendor request CVE IDs.

Without independent confirmation or vendor acknowledgement, it may not be possible to determine if the vulnerability is real, which could result in a request for a CVE ID being denied.

There are several documents that provide guidelines on disclosure. See Appendix A: Documents on Disclosure Practices for more details.

In general, you should do the following:

1. Find and notify the appropriate security contact for the vendor. If you cannot find a contact, try technical support.
2. Allow the vendor five business days to respond and acknowledge that they are aware of the problem. An “auto-reply” email or other computer-generated response does not represent vendor awareness.
    a) Work with the vendor to explain the problem, conduct further analysis if necessary, test any patches that the vendor proposes, and ensure the accuracy of both your, and the vendor’s, advisory.
3. If, after five business days, the vendor is unresponsive, report the problem to a third party “coordinator” such as CERT/CC. These coordinators may have contacts with the vendor, or they may lend credibility to your report.
4. If an advisory will not be published by the vendor or an established response team (e.g., CERT/CC), you may choose to announce the vulnerability to a public forum that allows others to validate the claims. Currently, those forums include the Bugtraq and Full-Disclosure mailing lists, and sites such as exploit-db and Packet Storm.

When possible, do not announce a vulnerability until the vendor has provided a patch. This could take between one day and six months, depending on the vendor and the nature of the problem. If you believe that the issue is urgent and the vendor is not responding quickly enough, try using a coordinator as described in #4. Also, you should avoid releasing precise details of the vulnerability until system administrators have time to apply the patch.

# 3. Requests to a vendor CNA

Software vendors participating as CNAs assign CVE IDs for their products. If the vulnerability is related to a CNA product, contact the appropriate CNA organization directly. If the request is accepted, the organization will assign a CVE ID for the issue and include it in its initial public announcement.

# 4. Requests to third party coordinator CNAs or e-mail lists

If a CVE ID cannot be requested through a CNA, consider contacting a third party coordinator such as an emergency response or vulnerability analysis team (e.g., CERT/CC), especially when there are problems in contacting the affected vendor. If the request is accepted, that organization will work to have a CVE ID assigned to the issue. Or, you may post the information to mailing lists such as BugTraq or oss-security and, if accepted, the issue will eventually be assigned a CVE ID by a CNA.

# 5. Requests to MITRE

If you are unable to obtain a CVE ID via the methods cited above, you may request a CVE ID directly from MITRE using MITRE's CVE Request web form (view guidance). Complete the "Request a CVE ID" web form.

Determine if the affected product is within the scope of MITRE as a CNA by checking the CVE Coverage Goals. If a product is not within scope, it may not be issued a CVE ID by the MITRE CVE Assignment Team.

As an exception, the MITRE CVE Assignment Team assigns CVE IDs for products that have been packaged by a Linux distribution on our Product List, such as Debian or Fedora. It is not necessary for the specific product name to be listed on the Product List.

CVE IDs are not assigned by the MITRE CVE Assignment Team for software that may be optionally added to a listed product, such as a third-party plugin or module. For example, CVE IDs are assigned for the WordPress core product, but not for any WordPress plugin. CVE IDs are also not assigned for Android or iOS apps unless the app's author is a listed vendor.

In addition, the MITRE CVE Assignment Team assigns CVE IDs for a number of programming languages including Python and PHP, but not for all code written in those languages. As an example, CVE IDs are not assigned for a web application written in PHP, unless the product or vendor is separately listed.

# 6. Information to provide in the request to MITRE

The CVE Request web form > Request a CVE ID requires 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; and
- The affected product and version for each vulnerability (a generic name can be used if the vulnerability has not been made public).

The required information is the minimum information required to request a CVE ID. However, you can also provide optional information which can be used to provide additional detail for your CVE ID request and may be valuable to creating the CVE entry as well as for downstream consumers.

Optional information includes:

- Attack type;
- Impact;
- Affected component;
- Attack vector;
- Discoverer;
- References; and
- Any additional information.

# 7. Confirmation of request

Upon completion of the CVE Request web form, the requestor will receive a confirmation email that the request was received and a reference number. If you need to communicate with MITRE about this request, reply to the confirmation email without changing the subject line, as it contains the reference number associated with your request.

If you do not seem to have received a confirmation email, please check your spam folder.

# 8. Follow-up information requests from MITRE

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

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

Once there is enough information to confirm the vulnerability exists and that it affects a covered product, the MITRE CVE Assignment Team will reply to the requester with a CVE ID. The CVE ID is considered “reserved” at this stage. Descriptions with details of the vulnerability will only be added when the vulnerability is made public (see step 12).

If the vulnerability is not confirmed, or if it is not in a covered product, a CVE ID request may be rejected. In this case, the requester will receive a response from the MITRE CVE Assignment Team notifying them of the decision.

# 10. Sharing the CVE ID with others

Once a CVE ID is obtained, provide it to all affected vendors and other parties (such as CERT/CC) with whom you are communicating. 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.

# 11. Information to include in a vulnerability announcement

When publishing a vulnerability with an associated CVE ID, include the CVE ID 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, which standardizes names for security problems.
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-YYYY-NNNN
- CVE ID: CVE- YYYY-NNNN

Some tips:

1. When announcing more than one CVE ID, associate each CVE ID with the vulnerability it is assigned to, 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

2. OSVDB offers additional suggestions about other content in the announcement:

   https://blog.osvdb.org/2013/01/15/researcher-security-advisory-writing-guidelines

# 12. Notify the MITRE CVE Assignment Team of publication

After your announcement has been publicized, contact the MITRE CVE Assignment Team by either replying to the original email discussion or via the CVE Request web form. 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, only a reserved CVE entry may be recorded on the CVE web site. No description or details of the vulnerability will be made available in the CVE entry until the vulnerability has been publicized.

When notified of a publication, MITRE will then populate the CVE entry with a description and references. This information will be made available on the CVE List.

The CVE information will also be updated in the National Vulnerability Database (NVD).

# Appendix A: Documents on disclosure practices

The following documents describe processes and provide guidelines for responsible 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

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: Determining if CVE IDs are needed

There are several factors to consider to determine whether one or more vulnerabilities require a CVE ID when providing information to MITRE :

A. Duplicates. Duplicates may be found by searching the MITRE CVE site and also by general web searches. Also, if a researcher previously contacted another organization on the CNA list about a vulnerability, a CVE ID assignment may already exist. The vulnerability should not be duplicated by the assignment of two CVE IDs.

B. Origination. CVE IDs are assigned to issues for which the primary method of addressing the vulnerability is for the vendor to take an action to remediate the vulnerability in their product. CVE IDs are not for cases in which the primary method of addressing the vulnerability is for an action to be taken by the operator of a single website or online service.

C. Establishing a policy violation. CVE IDs are needed when the vendor agrees that the observed product behavior violates a security policy, such as an unintended loss of confidentiality, integrity, or availability. CVE IDs are not for cases in which a reporter unilaterally believes that product hardening is desirable, such as a different approach to abuse prevention, or a different display of security-relevant data.

D. Establishing whether the vulnerabilities differ. In cases of multiple findings reported at the same time for a single product, separate CVE IDs are sometimes needed when there is a difference in the primary vulnerability types or affected versions.

E. Cross-vendor coordination. Separate CVE IDs are not assigned solely because vulnerable code is shipped in more than one product. Particularly in the case of open-source software, it is common for multiple vendors to use the same CVE ID in any scenario in which they have bundled, repackaged, or copied a piece of vulnerable code.

# Appendix C: 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:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1

mQINBFb1cyYBEAC6z0QzTNhnlyTnBRjOOH2m84gVibf5+S19pY985uaseeeZoWelBiLCQKvc
ecUotSfugtVEfJScvtom4/FnQgpzYqseEM46CVKdQRNqU8tqqR/CXoUY8ceBB3X5sj+bbRZ4
seqlePawOExa8WEX8dyPJ2QDop9lLwYgsBadyvJuwrQetssMSGAriRoDipAkGkZ/bId/oGZo
y8xh1LGNXXWob4qFXsrqSNPYseJ1SHxTOVhZ2s49zEu5+Mb5JedhTyDvID5LetCM87fJUDvi
n+GI5L6/0LhlOKSJVxWaYCQtsJTmEKSPpICF+419Dnt/w/WPFWXpp62SaT4Z2W8F0ALqKYZA
ZGEk5e7Ax/YUPoDb1wGBH1/n5GczV8fduiTsT0bQKd+Z5d2kMOsEoq4x2HC4mJpzt+iYoY8q
LrzyR/DTfH7C67GJjXFpkqkHUOS6m3k4QuV7ffiOkMo9ji/UySXdb5eQBe3lKRonTsIVe54H
WI7Cq9AO2mpoyfgOAcKIlfRUxPIMiN3VY6IvBpD1X2Ybcg4j+h/2nAAap22er31CWIwjWoPd
sKgP7SR+wYAcQve8vmRBJY3VVBHBLypSWgvzCipIyr71od/s8/889JKw9Lg7rvdsGXYZ4Hmm
```

```
O09OzbJ3j1CJeFRHjGPTgDBaR9H2pqs9wpMFGpjuh2iapDSqdwARAQABtCtNSVRSRSBDVkUg
VGlja2V0aW5nIDxjdmUtcmVxdWVzdEBtaXRyZS5vcmc+iQI9BBMBCAAnBQJXu1czAhsDBQkD
wmcABQsJCAcDBRUKCQgLBRYCAwEAAh4BAheAAAoJEHb/MwWLVhi2AYcP/iC691geDd7KjggM
kJIAGaU0uXCerv/8fv6v8xf1mYiLQhTnKi7cbdTVdVviO/tHiXgWhqLPV6njdMr+lJtUhKxr
htWl3m49+x01CLXh+QvWyTV+Lu/q36IUMAG5ZqYq/sizelwuAiA38RE3kwfPGmtDVmF0VrjS
GHsVM6jbe1RPz55sb+G5MQ74eq77PRtTz+8xU9S5mqfPlERQrd/S0WTj3wyxbWDMzE3mBiTG
GHKr4ErEgIzCuwSspF3HmOFI0Pcd24+7lDAH4DrzoYSvPSOt76PVe2V1bW1S8Ecu4KSs5Qhj
zgxQ70IpfPDazoC0Z55QECLgigfWv9OJE8WP6aKv/crBZJfC8CYa07k8xDETiXVNmYVDPF/P
uRmyGUweya778Q4YovAcVpMHdliRLZHvk9o4AXIbzP9yCAmYiZXcRBwSotPgZKWnCuDqelFb
4AnAhXIb4Zj1dBRXAZYNrCvKlS4s2sVyZt5tFTlN8F1Q+jaJcykIZdoEUwyiTOOgaJ8hmBp4
IQ8oz55x4IH0aln1QkCfy3/yOHbjW/taG/1zgEfmB3AZuMxly5YI4BEdVeqo3opns1MG6aZI
x40KWkf95akkkkFeMYWUtc3xGeQs6KwGpaKQE3fdSrAkQMqzIZ9vsS8BKQ6Q6+epjS1QOmFz
5V79rKmYjxPFB3vQzr40iQIcBBABCAAGBQJXu1kjAAoJEL54rhJi8gl53KMP/idyudqG7AAE
Lz9Hh6Cfol/FFLu2kLYn3yjd06J5VNxvsQTgLAeowqs77dGFpU8C8IlyfO1FnaNaklXTNJu+
+duHMLZvOLlW3/SWB2N1+q5gK74XXEUwrFmguhI4BiWJSBzrq0+PSWhEfv5McW/V3Kf2Pyiw
xKrvqVzDrpPSLIaqRSqpvhxZr1JlS0CvumZ2IT9quW93d6QwwkpNAsvtGB/9y+/ZqeEPdyTC
8yPtff0tOmlY8HJLFhTriwS7Y+4cxa55qhFD8aubeUkrUhs8Lrr21Nli+VhOcV/aZAtU7pns
1pZ09Zk4fpHxbl3qSfY7r77KmR/Hqh4FY0HgFSq4UJ25RvqH0YBx3868Q//PTySZ0Kb66MV3
OcRllVw7F13Hvj8Ce4gqBTNpDgFyyzrg0iIERBPlZdXFLRKgg+/FHq8W00B0/zDnu3VhiHM1
Bo0hch+5S1bF8uAg4XhzFrgi/sIuokl77xMc0wzOYWujR3DDb6x/JSDzrlkilSzChZUUPcAP
8WtITg47Z0O6hrQrR5MSzOX4Aa5+GYo+DXfCglI3zAjnO4WlbS2Lz+NZez1DGd1cQP9LGAv7
rtnTF7w9dB8ulyYhiz90ZAkeL26PedE15Nljr8tt95dKqCpAbZPM6koqsPGdoNPFd5+crZTP
+S5sFK6eNROwjZfsR1uuh1mztDRNSVRSRSBDVkUgTnVtYmVyaW5nIEF1dGhvcml0eSA8Y3Zl
LWFzc2lnbkBtaXRyZS5vcmc+iQIcBBABCAAGBQJXEQ+AAAoJEL54rhJi8gl5mbYP/jzbkQQe
WE1o61zGDDvUuIsFHaN/tPCUSHF9nqkJlr+B6HL5xqaeygJeA01ZqYDGIbR6fU675X7d/DMH
ThsLDNnv0racAJDjnCvfynC500kCfnDbB9HPakmMJBg2r5lpsX+E3t6cX2ulGtTtzAf1/M/M
Gpd0jwYv4La/M1ZQ4AihVzL0ng6kqDVzA2bqrsj8FH6l/KiPBRLmuCro+41aEuJzbkFfrtoP
2u7oMJ/8QNXoqPIbfgK0QUUQ24BBJAwPEh8m1genjv5uiO1wpECjr1nEgQIFYXmqpoI/a0nG
ujlmzwihGbfVRH9BlPQU0S349++QJ8Bgz24PMGplCmFFJzLKKURBY2Jk/BAidBJibar690vu
pDNTjsBedfDP6TjE5xaiKfxBl86+l37NyfkyAqst1/jGSJ3BekZt60e+HLsx2/BV4AHjdbIq
sZrF129bmzyOo2uS9uDKzQv+WijNj1GUpV7lEJheEBMqwywUn9k7w+V2dbOWHCPcPemFsDIi
9EnAT+wnqZy0yvXz++qrnOTn9hOuB/lRbrHPS4+C5DbeEWZ1IF7Rm5RpaUMV5SmISaAW9crc
sWyoVUL/JK39s91fOlj+2nww8IS2eY12LbKSKsUX89rWYziIt+nCDjGKdMir5cOLuV3DEZt8
b4pw0COVNW2AiwhNtXdGx5EZxgZWiQI9BBMBCAAnBQJW9XMmAhsDBQkDwmcABQsJCAcDBRUK
CQgLBRYCAwEAAh4BAheAAAoJEHb/MwWLVhi2F9kP/23uRw8lsNkdgTTvNAhVJAfhmDi7XrCd
H4WxeS4PJbjoTuqVbPonYOpv+XvPqj6tLO+lrHIFTksjGX5eiJJz2DN/XUCgf1eqEwbt3TM+
3r4ijwI+O2QVtlNBpm3rTPoQuYA1TQdDuPaqLigLnV0O1vlD3b6TD0yzVifY9A5IzOABGSLV
gT4lcTrt/d+FIjwKKMfir+IE1SVn3N7KqeP6F2mPmyjCzB8vNqqImAVUjpHnDAMpb5/GfB3l
wFvccjs/UwY+UND/7e4eoOjIcDTcvitDEtRGd1mTM7qIMbJx61c9DnDsrbJ1ngZetN73720m
cc7O/NhHKViQlGnzkIf6dG0tMuZReqSkgMoNYgofwd75lN5M1UJhW5ZqsdJwj5+VeGhDq7PW
phkztEzYANfnjWJUAGfu0IZPGtQjm2NgJmJL1GqiHoGqBLM/wSD1MzCiUxve4ff1PjSR+wyK
R+OMHtpnSxIHklBp96rAIAFj8l7aiicGyfK5Rcn9OHIe90a0OmBSxDGwPAO1xfYdJ4Tb5Iwr
QPjgMje9hYRRag4DRnnQwEZ8etXEDFSq/gR/WvH6HuP5M3UedVUwamxcd4OBq93wMn8v7j1R
CbrTvLSuHWkGASYrv4xnnY0DM5jhn59Y+1TvEpPDxW1KTg5ud5KyeMYmYwYYrPmHVbuY3lVi
d05SuQINBFb1cyYBEADEJoQRiuO8i3uPSy1ORnUZoRU35wrxjsxI7J6cupd6DINrmU8KGb6H
pHEFmNjOlylax5OogvsvgnmqxfAhlpVi7rw/R17ZtYpikiW7kle+9JXW4A8vY77hDizMfVF9
r/7e6yU2Dz1XCHvo1heBcAx4EiBNpvuEzPaBOIOMdBRMLS70Ke7+CyfuFXr4MW/ff3L18BO7
wENaljkVwWpvGIwAX7s+dnezX2g474HG6aiLJ6qJrXs1EiP9lT3XaT4Gmjlx1iN/J/BSlVCy
SmknpPoithSMLMsllILTqfcWYt/7hubM1CdM+O3uJ/TJ3YtYLV13fPvyK4ud0zJPrY/kPZ0O
XsxzHM8fGgMh2H47CCvTmdjjoP8x+PCbsz5eoB4lGhENEBQcxMcs96h292wQLRiq64qKtKcz
zeXwTFWeAJNBWfry25vY4r3Hhx2DCFD81+Q6VPnggIxC8X+ukRN8KX5+/ZueN4HHZ/SMsQ9Y
xIo4giJZRhYhpDP2Rgn1HQHxRwZVLqE1CwIkNWT1soUxS/jzFOqcgUCtAsvN7YnBgQepUgMW
YPxFl0W53VWFVFPBaMtUsW3MbnEWtWzGtgClnZJ8qfyW2bbCLdoyYOVjeOgGLHRj0gnjpTcV
VoatdczhETAexOGpQp2QWPkXfO5e0KkpUq4vd9fgYHDfruNFWOdzWwARAQABiQIlBBgBCAAP
BQJW9XMmAhsMBQkDwmcAAAoJEHb/MwWLVhi2TcMP/jR9byV+5vxQaY+Nu+6rdwvHYdj8+tLX
x3EfYRkbO3X57bNJtwUBScBYf47Gbhz9WJTnJHzQQ51gh3obc21do8thmf/LiEswuis3AYLX
Hf9qVFDt/VjeCd51ftDLG3zqB1R2y8nJ52ZQjctiYIuXMWornbhrPu2EVJZN4+m7a7HKYt5o
qLwQSiPk0ZgH7mP/Cc8HLZduwxIatTvtDumIjinKsrsVjVFpdmfuROYKzMvukggn3sHSMC6B
6epejv+Pt8hxR7oEJRTXfTwyVNcL7NFfy/A1e0XNxDtC6b2jIb8nWlPLYF1cRqXXyOqa1i7B
NQOaAq+zLDmSB47WxqWXbZCmKZ+7LWFQwhjQlKGDTkKebcbMCwq7Blztm8lz6wiCy/zm4V3s
Rt+u2k7dyfCrKNXMF9KwqurpoW2tGtdR+TlexQatp5FAC2bzgAHcn9eoAMO+f48sFG/+4DS/
CnMPPpU96uymTtsxjPO7Gc6+nIBzovUueKZRrdltXAaC9Dbq6RIZ1mCCKf0aNWky2DwWEkyw
n6FCs6iXtDg0xIu1L1l+ZDDGg++ZGlDwL9kkgvz/ObC5XEO61TMH7K8bAHueLTQMyHYpMez5
h9Vrait+I9pujWMoAlHoXFu2j6eCeyygrwAhJTB84JbBetEn+Q+fZqv7ly50iASzXLR8utBc
Adbk
=rTcK
-----END PGP PUBLIC KEY BLOCK-----
```

(NOTE: PGP key updated August 2016)