**Prepare – Consult a lawyer!**

* define the scope
* check if company has
  + identified security contacts: typical security@, abuse@, noc@ ([RFC2142](https://www.ietf.org/rfc/rfc2142.txt)) or [public](https://first.org/members/teams/) [CERT](https://www.trusted-introducer.org/directory/teams.html).
  + a responsible disclosure web page
  + bug bounty program. Example platforms : hackerone, bugcrowd, synack, bountyfactory.io...
  + a security.txt file on one of their websites ([website](https://securitytxt.org/), [github repo](https://github.com/securitytxt/security-txt" \t "_blank), [ietf draft](https://www.ietf.org/id/draft-foudil-securitytxt-00.txt" \t "_blank))

**Identify**

Remember if they are rules defined by a bounty program or laws applied to your country. Document every step allowing to identify vulnerability, and if acceptable in your context, how to exploit it.

**Report**

It is recommended to use responsible disclosure when dealing with vulnerabilities

* alert the company, multiple times and persons if needed.
* request [CVE Identification](http://cve.mitre.org/cve/request_id)([RedHat CVE HowTo](https://github.com/RedHatProductSecurity/CVE-HOWTO)).
* alert trusted 3rd party like National CERT, Data Privacy regulator if apply. Eventually, some security researchers like [Brian Krebs](https://krebsonsecurity.com/) or [Troy Hunt](https://www.troyhunt.com/) (non-exhaustive. check your network first) can be intermediate too or provide support.
* full/public disclosure

Depending on your context, each step may have more or less important time interval. Be flexible. ***Encourage trust, transparency and openness***. Timeline of full disclosure is always a debate especially if there is active exploitation. Be considerate of the work necessary to do the fix while balancing with public interest.

Examples of public disclosure timeline and methodology

* RFPolicy, Rain Forest Puppy, 2000: [5d](https://dl.packetstormsecurity.net/papers/general/rfpolicy-2.0.txt) for initial contact
* Google Project Zero:
  + [90d](https://googleprojectzero.blogspot.ca/2015/02/feedback-and-data-driven-updates-to.html) after initial notification and 14d grace period
  + [7d after if actively exploited Microsoft, 2016](https://www.secpod.com/blog/google-discloses-zero-day-in-windows-kernel/)
* US CERT/CC: [45d](https://www.cert.org/vulnerability-analysis/vul-disclosure.cfm) after initial report
* Internet Engineering Task Force (IETF): [Responsible Vulnerability Disclosure Process](https://tools.ietf.org/html/draft-christey-wysopal-vuln-disclosure-00). Insisted on joined work with no unique timeline
* Microsoft: [Coordinated Vulnerability Disclosure](https://technet.microsoft.com/en-us/security/dn467923) (CVD)
* ISO/IEC [29147:2014](http://www.iso.org/iso/catalogue_detail.htm?csnumber=45170): Vulnerability disclosure

Report should include all details necessary to understand vulnerability and reproduce it (exploit code for example). If you identify limiting factors, include them (Non-Admin user, use of Ms EMET, security HTTP headers...).

If possible, use encryption like PGP/GPG to encrypt your report. You can use [Encrypt.to](https://encrypt.to/) to do from a web browser if recipient has a public key. If you want to remain anonymous, it's probably better to use pseudonym and one-time use email on Tor network or similar. Intermediate party might also be available like ZeroDisclo.com but ensure target destination is relevant (In 2017, mostly FR & EU).

**Aftermath**

If you think your lessons learned would be useful to community, share it (anonymously or not).

**Legal**

Most western countries have an exception for interoperability and security research but...

* US: Sec. 103(f) of the DMCA (17 U.S.C. § 1201 (f)) but EULA and contract override law.
* FR: [Art.](https://fr.wikipedia.org/wiki/R%C3%A9tro-ing%C3%A9nierie#L.C3.A9gislation) [L. 335-3-1 - article 22 du DADVSI](https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000266350&categorieLien=id) (2006), [EU Directive 2009/24](http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32009L0024)
* CA: Ambiguous... Bill [C-32](http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=4580265&Language=e&Mode=1) (2010), Bill [C-11](http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=5465759) (2011). Criminal code provisions (Bill [C-46](http://laws-lois.justice.gc.ca/eng/acts/C-46/FullText.html)) for testing without permission: 430(1.1) ("Mischief in relation to computer data"), 342.1 ("Unauthorized use of a computer"), 342.2 ("Possession of device to obtain unauthorized use of computer system or to commit mischief").

**Definitions**

* Full disclosure

*Full disclosure is the practice of publishing analysis of software vulnerabilities as early as possible, making the data accessible to everyone without restriction. The primary purpose of widely disseminating information about vulnerabilities is so that potential victims are as knowledgeable as those who attack them.*, [Wikipedia](https://en.wikipedia.org/wiki/Full_disclosure_%28computer_security%29)

* Responsible disclosure

*The issue is reported privately to the vendor and no one else until the vendor issues a patch.*, [Microsoft](https://www.microsoft.com/en-us/msrc/cvd), 2010

* Coordinated disclosure

*Coordinate public release happens, ideally, when the vendor releases the update. In the case of publicly verifiable active attacks, details may be released prior to an update being released, with emphasis on giving details to protection providers.*, [Microsoft](https://www.microsoft.com/en-us/msrc/cvd), 2010

* Private disclosure

*The vulnerability is released to a small group of people (not the vendor) or kept private.*

Other definitions : [CERT/CC](https://vuls.cert.org/confluence/pages/viewpage.action?pageId=4718642)

CNAs are listed alphabetically:

|  |  |  |  |
| --- | --- | --- | --- |
| Product, Vendor, or Product Category Name | Scope | CNA Contact Email and/or Webpage (if applicable) | CNA Type\* |
| MITRE Corporation | All vulnerabilities, and Open Source software product vulnerabilities, not already covered by a CNA listed on this page | [MITRE CVE Request web form](https://cveform.mitre.org/) | Program Root CNA |
|  |  |  |  |
|  |  |  |  |
| Adobe Systems Incorporated | Adobe issues only | [psirt@adobe.com](mailto:psirt@adobe.com)  [Adobe security page](https://helpx.adobe.com/security/alertus.html) | Vendors and Projects |
| Airbus | All Airbus products (supported products and end-of-life/end-of-service products), as well as vulnerabilities in third-party software discovered by Airbus that are not in another CNA’s scope | [vuln@airbus.com](mailto:vuln@airbus.com)  [Airbus Vulnerability Handling and Disclosure](https://www.airbus.com/contact-us.html) | Vendors and Projects  Vulnerability Researchers |
| Alibaba, Inc. | Projects listed on its [Alibaba GitHub website](https://github.com/alibaba) only | [alibaba-cna@list.alibaba-inc.com](mailto:alibaba-cna@list.alibaba-inc.com)  [Alibaba website](https://www.alibaba.com/)  [Alibaba GitHub website](https://github.com/alibaba) | Vendors and Projects |
| Android (associated with Google Inc. or Open Handset Alliance) | Android issues only | [security@android.com](mailto:security@android.com)  [Android security page](https://www.google.com/about/appsecurity/android-rewards/) | Vendors and Projects |
| Apache Software Foundation | All Apache Software Foundation issues | [security@apache.org](mailto:security@apache.org)  [Apache security page](https://www.apache.org/security/) | Vendors and Projects |
| Apple Inc. | Apple issues only | [product-security@apple.com](mailto:product-security@apple.com)  [Apple security page](https://www.apple.com/support/security/) | Vendors and Projects |
| Appthority | All Appthority products, as well as vulnerabilities in third-party software discovered by Appthority that are not in another CNA’s scope | [security@appthority.com](mailto:security@appthority.com)  [Appthority Disclosure Policy](https://www.appthority.com/legal/vulnerability-disclosure-policy/)  [Appthority Advisories](https://www.appthority.com/mobile-threat-center/advisories/) | Vendors and Projects  Vulnerability Researchers |
| Asea Brown Boveri Ltd. (ABB) | ABB issues only | [cybersecurity@ch.abb.com](mailto:cybersecurity@ch.abb.com)  [ABB Disclosure Policy](https://library.e.abb.com/public/71f0c85561b7448498bd765c65ce54fc/9ADB005059_ABB_SoftwareVulnerabilityWhitepaper_RevE.pdf?x-sign=IO082OW/SNgyOLcAZmwQdgcFxTiqMdgoaZze1sLMNIeSVSsSgD1CltJarfNb5GkL)  [ABB Advisories](https://new.abb.com/about/technology/cyber-security/alerts-and-notifications) | Vendors and Projects |
| Atlassian | All Atlassian products, as well as Atlassian-maintained projects hosted on <https://bitbucket.org/atlassian> and <https://github.com/atlassian/> | [security@atlassian.com](mailto:security@atlassian.com) | Vendors and Projects |
| Autodesk | [All currently supported Autodesk Applications and Cloud Services](https://knowledge.autodesk.com/support) | [psirt@autodesk.com](mailto:psirt@autodesk.com) | Vendors and Projects |
| Avaya, Inc. | All Avaya products | [securityalerts@avaya.com](mailto:securityalerts@avaya.com)  [Avaya Disclosure Policy](https://downloads.avaya.com/css/P8/documents/100045520)  [Avaya Advisories](https://support.avaya.com/security) | Vendors and Projects |
|  |  |  |  |
| Bitdefender | All Bitdefender products, as well as vulnerabilities in third-party software discovered by Bitdefender that are not in another CNA’s scope | [cve-requests@bitdefender.com](mailto:cve-requests@bitdefender.com)  [Bitdefender Disclosure Policy](https://www.bitdefender.com/media/materials/bug_bounty/Bitdefender_Bug_Bounty_Terms_and_Conditions.pdf)  [Bitdefender Advisories](https://www.bitdefender.com/support/security-advisories/) | Vendors and Projects  Vulnerability Researchers |
| BlackBerry | BlackBerry and Good product issues only | [secure@blackberry.com](mailto:secure@blackberry.com)  [Blackberry security page](https://global.blackberry.com/en/secure/report-an-issue/en) | Vendors and Projects |
| Robert Bosch GmbH | Bosch products only | [psirt@bosch.com](mailto:psirt@bosch.com)  [Bosch Disclosure Policy](https://psirt.bosch.com/en/responsibleDisclosurePolicy.html)  [Bosch Advisories](https://psirt.bosch.com/index.html) | Vendors and Projects |
| Brocade Communications Systems, LLC | Brocade products only | [brocade.sirt@broadcom.com](mailto:brocade.sirt@broadcom.com)  [Brocade security page](https://www.broadcom.com/support/fibre-channel-networking/security-advisories) | Vendors and Projects |
|  |  |  |  |
| Canonical Ltd. | All Canonical issues (including Ubuntu Linux) only | [security@ubuntu.com](mailto:security@ubuntu.com)  [Ubuntu security page](https://wiki.ubuntu.com/SecurityTeam/FAQ#Contact) | Vendors and Projects |
| CA Technologies - A Broadcom Company | CA Technologies issues only | [ca.psirt@broadcom.com](mailto:ca.psirt@broadcom.com)  [CA Technologies Disclosure Policy](https://techdocs.broadcom.com/us/product-content/recommended-reading/security-notices/contact-information-for-ca-product-vulnerability-response-team.html)  [CA Technologies Advisories](https://techdocs.broadcom.com/us/product-content/news/vulnerability-alerts/vulnerability-alerts---view-all.html) | Vendors and Projects |
| CERT/CC | Vulnerability assignment related to its vulnerability coordination role | [cert@cert.org](mailto:cert@cert.org)  [CERT/CC contact page](https://vulcoord.cert.org/VulReport/) | National and Industry CERTs |
| Check Point Software Technologies Ltd. | Check Point Security Gateways product line only, and any vulnerabilities discovered by Check Point that are not in another CNA’s scope | [cve@checkpoint.com](mailto:cve@checkpoint.com) | Vendors and Projects  Vulnerability Researchers |
| Cisco Systems, Inc. | All Cisco and Duo Security products, and any third-party research targets that are not in another CNA’s scope | [psirt@cisco.com](mailto:mailto:psirt@cisco.com)  [Cisco Disclosure Policy](https://www.cisco.com/c/en/us/about/security-center/security-vulnerability-policy.html)  [Cisco Advisories](https://tools.cisco.com/security/center/resources/security_vulnerability_policy.html#sa)  [psirt@duosecurity.com](mailto:mailto:psirt@duosecurity.com)  [Duo Security Disclosure Policy](https://duo.com/labs/disclosure)  [Duo Security Advisories](https://duo.com/labs/psa/) | Vendors and Projects  Vulnerability Researchers |
| Cloudflare, Inc. | All Cloudflare products, projects hosted at <https://github.com/cloudflare/>, and any vulnerabilities discovered by Cloudflare that are not in another CNA’s scope | [cna@cloudflare.com](mailto:cna@cloudflare.com)  [Cloudflare Disclosure Policy](https://www.cloudflare.com/disclosure/)  [Cloudflare Advisories](https://hackerone.com/cloudflare/hacktivity) | Vendors and Projects |
| CyberSecurity Philippines - CERT | Vulnerability assignment related to its vulnerability coordination role that are not in another CNA’s scope | [vulnerability@cspcert.ph](mailto:vulnerability@cspcert.ph)  [CyberSecurity Philippines - CERT Disclosure Policy](https://www.cspcert.ph/policy.html)  [CyberSecurity Philippines - CERT Advisories](https://www.cspcert.ph/advisories.html) | National and Industry CERTs |
|  |  |  |  |
| Dahua Technologies | Dahua issues only | [cybersecurity@dahuatech.com](mailto:cybersecurity@dahuatech.com)  [Dahua security page](http://www.dahuasecurity.com/en/us/cybersecurity.php) | Vendors and Projects |
| Debian GNU/Linux | Debian issues only | [security@debian.org](mailto:security@debian.org)  [Debian security page](https://www.debian.org/security/) | Vendors and Projects |
| Dell | Dell, Dell EMC, RSA, and VCE issues only | [secure@dell.com](mailto:secure@dell.com)  [Dell Disclosure Policy](https://www.dell.com/support/contents/us/en/04/article/product-support/self-support-knowledgebase/security-antivirus/alerts-vulnerabilities/dell-vulnerability-response-policy)  [Dell Advisories](https://www.dell.com/support/security/en-us/) | Vendors and Projects |
| Document Foundation, The | Projects within The Document Foundation only, e.g., LibreOffice, LibreOffice Online; The Document Foundation discourages reporting denial of service bugs as security issues | [security@documentfoundation.org](mailto:security@documentfoundation.org)  [The Document Foundation Disclosure Policy](https://www.libreoffice.org/about-us/security)  [The Document Foundation Advisories](https://www.libreoffice.org/about-us/security/advisories/) | Vendors and Projects |
| Drupal.org | All projects hosted under drupal.org only | [security@drupal.org](mailto:security@drupal.org)  [Drupal security advisories page](https://www.drupal.org/drupal-security-team/security-advisory-process-and-permissions-policy) | Vendors and Projects |
|  |  |  |  |
| Eaton | Eaton issues only | [cybersecuritycoe@eaton.com](mailto:cybersecuritycoe@eaton.com)  [Eaton Disclosure Policy](https://www.eaton.com/us/en-us/company/news-insights/cybersecurity/vulnerabilitydisclosure.html=20)  [Eaton Advisories](https://www.eaton.com/us/en-us/company/news-insights/cybersecurity/security-notifications.html) | Vendors and Projects |
| Eclipse Foundation | Eclipse IDE and the Eclipse Foundation's eclipse.org, polarysys.org, and locationtech.org open source projects only | [security@eclipse.org](mailto:security@eclipse.org)  [Eclipse security page](https://www.eclipse.org/security) | Vendors and Projects |
| Elastic | Elasticsearch, Kibana, Beats, Logstash, X-Pack, and Elastic Cloud Enterprise products only | [security@elastic.co](mailto:security@elastic.co)  [Elastic security page](https://www.elastic.co/community/security) | Vendors and Projects |
|  |  |  |  |
| F5 Networks | F5 issues only | [f5sirt@f5.com](mailto:f5sirt@f5.com)  [F5 Vulnerability Response Policy](https://support.f5.com/csp/article/K4602?) | Vendors and Projects |
| Facebook, Inc. | Facebook-supported open source projects, mobile apps, and other software, as well as vulnerabilities in third-party software discovered by Facebook that are not in another CNA’s scope; see: <https://www.facebook.com/whitehat> and <https://github.com/facebook/> | [Facebook security page](https://www.facebook.com/whitehat) | Vendors and Projects  Vulnerability Researchers |
| Fedora Project | Fedora Project issues only | [Fedora Bug Report page](https://fedoraproject.org/wiki/Bugs_and_feature_requests) | Vendors and Projects |
| Flexera Software LLC | All Flexera products, and vulnerabilities discovered by Secunia Research that are not in another CNA’s scope | [PSIRT-CNA@flexerasoftware.com](mailto:PSIRT-CNA@flexerasoftware.com) | Vendors and Projects  Vulnerability Researchers |
| floragunn GmbH | All issues related to Search Guard only | [security@search-guard.com](mailto:security@search-guard.com)  [floragunn Disclosure Policy](https://search-guard.com/disclosure-policy)  [floragunn Advisories](https://search-guard.com/cve-advisory) | Vendors and Projects |
| Forcepoint | Forcepoint products only | [psirt@forcepoint.com](mailto:psirt@forcepoint.com)  [Forcepoint security page](https://www.forcepoint.com/company/innovation/product-security-report-issue) | Vendors and Projects |
| Fortinet, Inc. | Fortinet issues only | [psirt@fortinet.com](mailto:psirt@fortinet.com) | Vendors and Projects |
| FreeBSD | Primarily FreeBSD issues only | [secteam@freebsd.org](mailto:secteam@freebsd.org) | Vendors and Projects |
|  |  |  |  |
| GitHub, Inc. | All libraries and products hosted on github.com in a public repository, unless they are otherwise covered by another CNA | [security-advisories@github.com](mailto:security-advisories@github.com)  [GitHub Disclosure Policy](https://help.github.com/en/articles/about-maintainer-security-advisories)  [GitHub Advisories](https://github.com/advisories) | Vendors and Projects |
| Google Inc. | Chrome and Chrome OS issues, and projects that are not in another CNA’s scope | Report vulnerabilities: [security@chromium.org](mailto:security@chromium.org)  Questions about Google’s CVE Entries: [chrome-cve-admin@google.com](mailto:chrome-cve-admin@google.com)   [Google app security page](https://www.google.com/about/appsecurity/) | Vendors and Projects |
|  |  |  |  |
| HackerOne | Provides CVE IDs for its customers as part of its bug bounty and vulnerability coordination platform | [support@hackerone.com](mailto:support@hackerone.com)  [HackerOne contact page](https://hackerone.com/) | Bug Bounty Programs |
| Hangzhou Hikvision Digital Technology Co., Ltd. | All [Hikvision Internet of Things (IoT) products](http://www.hikvision.com/en/product_1.html) including cameras and digital video recorders (DVRs) | [hsrc@hikvision.com](mailto:hsrc@hikvision.com) | Vendors and Projects |
| HCL Software | All HCL products only | [psirt@hcl.com](mailto:psirt@hcl.com)  [HCL Disclosure Policy](https://www.hcltech.com/software/psirt/hcl-software-vulnerability-disclosure-policy)  [HCL Advisories](https://hclpnpsupport.hcltech.com/csm?id=search&spa=1&t=kb&q=Security%20Bulletin) | Vendors and Projects |
| Hewlett Packard Enterprise (HPE) | HPE issues only | [security-alert@hpe.com](mailto:security-alert@hpe.com) | Vendors and Projects |
| Hillstone Networks, Inc. | All [Hillstone products](https://www.hillstonenet.com/products/) only | [sec@hillstonenet.com](mailto:sec@hillstonenet.com)  [Hillstone Disclosure Policy](https://www.hillstonenet.com.cn/product-and-service/security-sevice/security-incident-response/)  [Hillstone Advisories](https://www.hillstonenet.com.cn/product-and-service/security-sevice/security-bulletins-and-advisories/) | Vendors and Projects |
| HP Inc. | HP Inc. issues only | [hp-security-alert@hp.com](mailto:hp-security-alert@hp.com) | Vendors and Projects |
| Huawei Technologies | Huawei issues only | [psirt@huawei.com](mailto:psirt@huawei.com)  [Huawei security page](https://www.huawei.com/psirt) | Vendors and Projects |
|  |  |  |  |
| IBM Corporation | All IBM products, as well as vulnerabilities in third-party software discovered by IBM X-Force Red that are not in another CNA’s scope | [psirt@us.ibm.com](mailto:psirt@us.ibm.com) | Vendors and Projects  Vulnerability Researchers |
| ICS-CERT | Infrastructure sector control systems | [ics-cert@hq.dhs.gov](mailto:ics-cert@hq.dhs.gov) | National and Industry CERTs |
| Intel Corporation | Intel branded products and technologies and Intel managed open source projects | [secure@intel.com](mailto:secure@intel.com)  [Intel security page](https://security-center.intel.com/) | Vendors and Projects |
| Internet Systems Consortium (ISC) | All ISC.org projects | [security-officer@isc.org](mailto:security-officer@isc.org)  [ISC report a bug page](https://www.isc.org/community/report-bug/) | Vendors and Projects |
|  |  |  |  |
| Jenkins Project | Jenkins and Jenkins plugins distributed by the Jenkins Project (listed on plugins.jenkins.io) only | [jenkinsci-cert@googlegroups.com](mailto:jenkinsci-cert@googlegroups.com)  [Jenkins Project Disclosure Policy](https://jenkins.io/security/)  [Jenkins Project Advisories](https://jenkins.io/security/advisories/) | Vendors and Projects |
| Johnson Controls | Johnson Controls products only | [productsecurity@jci.com](mailto:productsecurity@jci.com)  [Johnson Controls Disclosure Policy](https://www.johnsoncontrols.com/buildings/specialty-pages/product-security/vulnerability-reporting-and-disclosure)  [Johnson Controls Advisories](https://www.johnsoncontrols.com/buildings/specialty-pages/product-security/security-advisories) | Vendors and Projects |
| JPCERT/CC | Vulnerability assignment related to its vulnerability coordination role | [vultures@jpcert.or.jp](mailto:vultures@jpcert.or.jp)  [JPCERT/CC contact page](https://www.jpcert.or.jp/vh/index.html) | Root CNA  National and Industry CERTs |
| Juniper Networks, Inc. | Juniper issues only | [sirt@juniper.net](mailto:sirt@juniper.net)  [Juniper security page](https://www.juniper.net/us/en/security/report-vulnerability/) | Vendors and Projects |
|  |  |  |  |
| Kaspersky | Kaspersky B2C and B2B products, as well as vulnerabilities discovered in third-party software not in another CNA’s scope | [vulnerability@kaspersky.com](mailto:vulnerability@kaspersky.com) | Vendors and Projects  Vulnerability Researchers |
| KrCERT/CC | Vulnerability assignment related to its vulnerability coordination role | [vuln@krcert.or.kr](mailto:vuln@krcert.or.kr) | National and Industry CERTs |
| Kubernetes | Kubernetes issues only | [security@kubernetes.io](mailto:security@kubernetes.io)  [Kubernetes Disclosure Policy](https://kubernetes.io/security)  [Kubernetes Advisories](https://kubernetes.io/cve) | Vendors and Projects |
|  |  |  |  |
| Larry Cashdollar | Third-party products he researches | [larry0@me.com](mailto:larry0@me.com) | Vulnerability Researchers |
| Lenovo Group Ltd. | Lenovo general-purpose computers, software for general-purpose operating systems, mobile devices, enterprise storage, and networking products only | [psirt@lenovo.com](mailto:psirt@lenovo.com) | Vendors and Projects |
|  |  |  |  |
| MarkLogic Corporation | MarkLogic issues only | [security@marklogic.com](mailto:security@marklogic.com) | Vendors and Projects |
| McAfee | All McAfee products, as well as vulnerabilities in third-party software discovered by McAfee ATR that are not in another CNA’s scope | [security\_report@mcafee.com](mailto:security_report@mcafee.com)  [McAfee Advisories](https://www.mcafee.com/enterprise/en-us/threat-center/product-security-bulletins.html) | Vendors and Projects  Vulnerability Researchers |
| Micro Focus International | All Attachmate, Borland, Gwava, Micro Focus, NetIQ, Novell, and Serena products, as well as all former HP Enterprise software suites | [security@microfocus.com](mailto:security@microfocus.com)  [Micro Focus Disclosure Policy](https://www.microfocus.com/security)  [Micro Focus Advisories](https://www.microfocus.com/security) | Vendors and Projects |
| Microsoft Corporation | Microsoft issues only | [secure@microsoft.com](mailto:secure@microsoft.com)  [Microsoft security page](https://technet.microsoft.com/en-us/security/ff852094.aspx) | Vendors and Projects |
| MITRE Corporation | All vulnerabilities, and Open Source software product vulnerabilities, not already covered by a CNA listed on this page | [MITRE CVE Request web form](https://cveform.mitre.org/) | Program Root CNA |
| MongoDB, Inc. | MongoDB products only | [cna@mongodb.com](mailto:cna@mongodb.com)  [MongoDB Disclosure Policy](https://www.mongodb.com/security)  [MongoDB Advisories](https://www.mongodb.com/security) | Vendors and Projects |
| Mozilla Corporation | Mozilla issues only | [security@mozilla.org](mailto:security@mozilla.org)  [Mozilla security page](https://www.mozilla.org/en-US/security/advisories/) | Vendors and Projects |
|  |  |  |  |
| Naver Corporation | Naver products only, except Line products | [cve@navercorp.com](mailto:cve@navercorp.com)  [Naver Disclosure Policy](https://cve.naver.com/)  [Naver Advisories](https://cve.naver.com/) | Vendors and Projects |
| NetApp, Inc. | All NetApp products as well as projects hosted on [https://github.com/netapp](https://github.com/netapp/) | [security-alert@netapp.com](mailto:security-alert@netapp.com)  [NetApp security page](https://security.netapp.com/) | Vendors and Projects |
| Netflix, Inc. | Current versions of Netflix Mobile Streaming Application for iOS, Android, and Windows Mobile, plus all Netflix Open Source projects hosted on [https://github.com/Netflix](https://github.com/Netflix/) and [https://github.com/spinnaker](https://github.com/spinnaker/) | [security-report@netflix.com](mailto:security-report@netflix.com) | Vendors and Projects |
| Node.js | All actively developed versions of software developed under the Node.js project on [https://github.com/nodejs](https://github.com/nodejs/) | [cve-request@iojs.org](mailto:cve-request@iojs.org)  [Node.js security page](https://nodejs.org/en/security/) | Vendors and Projects |
| NVIDIA Corporation | NVIDIA issues only | [psirt@nvidia.com](mailto:psirt@nvidia.com)  [NVIDIA security page](https://www.nvidia.com/security) | Vendors and Projects |
|  |  |  |  |
| Objective Development Software GmbH | Objective Development issues only | [Objective Development security page](https://obdev.at/go/cna) | Vendors and Projects |
| Odoo | Odoo issues only | [security@odoo.com](mailto:security@odoo.com)  [Odoo Disclosure Policy](https://www.odoo.com/security-report)  [Odoo Advisories](https://www.odoo.com/security-advisories) | Vendors and Projects |
| OpenSSL Software Foundation | OpenSSL software projects only | [openssl-security@openssl.org](mailto:openssl-security@openssl.org)  [OpenSSL contact web page](https://www.openssl.org/news/vulnerabilities.html) | Vendors and Projects |
| Opera Software AS | Opera issues only | [Contact web page](https://security.opera.com/report-security-issue/)  [Opera Disclosure Policy](https://security.opera.com/policy/)  [Opera Advisories](https://security.opera.com/advisories/) | Vendors and Projects |
| OPPO Mobile Telecommunication Corp., Ltd. | OPPO devices only | [security@oppo.com](mailto:security@oppo.com)  [OPPO Disclosure Policy](https://security.oppo.com/disclosurePolicy.html)  [OPPO Advisories](https://security.oppo.com/) | Vendors and Projects |
| Oracle | Oracle Premier and Extended Support product versions per Oracle’s [Lifetime Support Policy](https://www.oracle.com/support/lifetime-support/index.html) | [secalert\_us@oracle.com](mailto:secalert_us@oracle.com)  [Oracle security page](https://www.oracle.com/support/assurance/vulnerability-remediation/reporting-security-vulnerabilities.html) | Vendors and Projects |
| OTRS AG | Vulnerabilities for OTRS and ((OTRS)) Community Edition and modules only | [security@otrs.com](mailto:security@otrs.com)  [OTRS Disclosure Policy](https://github.com/OTRS/otrs/blob/rel-6_0/SECURITY.md)  [OTRS Advisories](https://otrs.com/overview-release-notes-security-advisories/security-advisories/) | Vendors and Projects |
|  |  |  |  |
| Palo Alto Networks, Inc. | All Palo Alto Networks products, and vulnerabilities discovered by Palo Alto Networks that are not in another CNA’s scope | [psirt@paloaltonetworks.com](mailto:psirt@paloaltonetworks.com)  [Palo Alto Networks Disclosure Policy](https://www.paloaltonetworks.com/security-disclosure)  [Palo Alto Networks Advisories](https://securityadvisories.paloaltonetworks.com/) | Vendors and Projects  Vulnerability Researchers |
| PHP Group | Vulnerabilities in PHP code (code in <https://github.com/php/php-src>) only | [security@php.net](mailto:security@php.net)  [PHP Group Disclosure Policy](https://wiki.php.net/security)  [PHP Group Advisories](https://www.php.net/ChangeLog-7.php) | Vendors and Projects |
| Pivotal Software, Inc. | Pivotal, Spring, and Cloud Foundry issues only | [security@pivotal.io](mailto:security@pivotal.io)  [Pivotal Disclosure Policy](https://pivotal.io/security), [Cloud Foundry Disclosure Policy](https://cloudfoundry.org/security)  [Pivotal Advisories](https://pivotal.io/security), [Spring Advisories](https://spring.io/blog), [Cloud Foundry Advisories](https://cloudfoundry.org/security) | Vendors and Projects |
| Puppet | All Puppet products, as well as all projects on [https://github.com/puppetlabs](https://github.com/puppetlabs/) | [security@puppet.com](mailto:security@puppet.com)  [Puppet security page](https://puppet.com/docs/vulnerability-submission-process) | Vendors and Projects |
|  |  |  |  |
| QNAP Systems, Inc. | QNAP QTS, QES, and QVR products as well as its mobile apps and utilities | [security@qnap.com](mailto:security@qnap.com) | Vendors and Projects |
| Qualcomm, Inc. | Qualcomm and Snapdragon issues only | [product-security@qualcomm.com](mailto:product-security@qualcomm.com) | Vendors and Projects |
|  |  |  |  |
| Rapid7, Inc. | All Rapid7 products, and vulnerabilities discovered by Rapid7 that are not in another CNA’s scope | [cve@rapid7.com](mailto:cve@rapid7.com)  [Rapid7 security page](https://www.rapid7.com/disclosure/) | Vendors and Projects  Vulnerability Researchers |
| Red Hat, Inc. | Linux issues only | [secalert@redhat.com](mailto:secalert@redhat.com)  [Red Hat security page](https://access.redhat.com/security/team/contact) | Vendors and Projects |
|  |  |  |  |
| Salesforce, Inc. | Salesforce [products](https://trust.salesforce.com/en/trust-and-compliance-documentation/) only | [security@salesforce.com](mailto:security@salesforce.com)  [Salesforce Disclosure Policy](https://trust.salesforce.com/en/security/responsible-disclosure-policy/)  [Salesforce Advisories](https://trust.salesforce.com/en/security/security-advisories/) | Vendors and Projects |
| SAP SE | All SAP products | [cna@sap.com](mailto:cna@sap.com) | Vendors and Projects |
| Schneider Electric SE | All Schneider Electric products, including Proface, Pelco, APC, and Eurotherm | [cybersecurity@se.com](mailto:cybersecurity@se.com)  [Schneider Electric security page](https://www.schneider-electric.com/b2b/en/support/cybersecurity/report-an-incident.jsp) | Vendors and Projects |
| SICK AG | SICK AG issues only | [psirt@sick.de](mailto:psirt@sick.de)  [SICK Disclosure Policy](https://sick.com/psirt)  [SICK Advisories](https://sick.com/psirt#advisories) | Vendors and Projects |
| Siemens | Siemens issues only | [productcert@siemens.com](mailto:productcert@siemens.com)  [Siemens security page](https://www.siemens.com/cert) | Vendors and Projects |
| Snyk | Vulnerabilities in third-party products discovered by Snyk only | [report@snyk.io](mailto:report@snyk.io)  [Snyk Disclosure Policy](https://snyk.io/docs/security/#open-source-packages-disclosure-policy)  [Snyk Advisories](https://snyk.io/vuln/) | Vulnerability Researchers |
| SonicWall, Inc. | SonicWall issues only | [PSIRT@sonicwall.com](mailto:PSIRT@sonicwall.com)  [SonicWall Disclosure Policy](https://psirt.global.sonicwall.com/vuln-policy)  [SonicWall Advisories](https://psirt.global.sonicwall.com/vuln-list) | Vendors and Projects |
| Splunk Inc. | Splunk products only | [prodsec@splunk.com](mailto:prodsec@splunk.com)  [Splunk Disclosure Policy](https://www.splunk.com/page/securityportal)  [Splunk Advisories](https://www.splunk.com/page/securityportal) | Vendors and Projects |
| SUSE | All SUSE Enterprise products and openSUSE software | [security@suse.de](mailto:security@suse.de)  [SUSE Disclosure Policy](https://www.suse.com/security/)  [SUSE Advisories](https://www.suse.com/support/update/) [SUSE Advisories by CVE ID](https://www.suse.com/security/cve/) | Vendors and Projects |
| Symantec Corporation | Symantec issues only | [secure@symantec.com](mailto:secure@symantec.com)  [Symantec security page](https://www.symantec.com/security/) | Vendors and Projects |
| Synology Inc. | Synology issues only | [security@synology.com](mailto:security@synology.com)  [Synology security page](https://www.synology.com/en-global/support/security) | Vendors and Projects |
|  |  |  |  |
| Talos | Third-party products it researches | [talos-cna@cisco.com](mailto:talos-cna@cisco.com)  [Talos web page](https://talosintelligence.com/) | Vulnerability Researchers |
| Tenable Network Security, Inc. | Tenable products and third-party products they research not covered by another CNA | [vulnreport@tenable.com](mailto:vulnreport@tenable.com)  [Tenable security page](https://www.tenable.com/security/report/) | Vendors and Projects |
| 360 Security Technology, Inc. | 360 Total Security, 360 Safeguard, 360 Mobile Safe, and 360 Safe Router products, and vulnerabilities in third-party products discovered by 360 that are not covered by another CNA | [security@360.cn](mailto:security@360.cn)  [360 Disclosure Policy](https://security.360.cn/en/policy.html)  [360 Advisories](https://security.360.cn/en/advisory.html) | Vendors and Projects  Vulnerability Researchers |
| TIBCO Software Inc. | TIBCO, Talarian, Spotfire, Data Synapse, Foresight, Kabira, Proginet, LogLogic, StreamBase, JasperSoft, and Mashery products/brands only | [security@tibco.com](mailto:security@tibco.com) | Vendors and Projects |
| Tigera, Inc. | All vulnerabilities for Calico and all of Tigera’s products only | [psirt@tigera.io](mailto:psirt@tigera.io)  [Tigera Disclosure Policy](https://www.projectcalico.org/vulnerability-disclosure/)  [Tigera Advisories](https://www.projectcalico.org/security-bulletins/) | Vendors and Projects |
| Trend Micro, Inc. | Trend Micro [supported products](https://success.trendmicro.com/solution/1105726-supported-products-trend-micro) and [end-of-life products](https://success.trendmicro.com/solution/1105727-list-of-end-of-life-eol-end-of-support-eos-trend-micro-products) issues only | [security@trendmicro.com](mailto:security@trendmicro.com)  [Trend Micro security page](https://success.trendmicro.com/vulnerability-response) | Vendors and Projects |
| TWCERT/CC | Vulnerability assignment related to its vulnerability coordination role | [cve@cert.org.tw](mailto:cve@cert.org.tw)  Chinese: [TWCERT/CC Disclosure Policy](https://twcert-official-file.s3.hicloud.net.tw/CNA/TWCERTCC%E6%BC%8F%E6%B4%9E%E6%8F%AD%E9%9C%B2%E6%94%BF%E7%AD%96.pdf) [TWCERT/CC Advisories](https://twcert.org.tw/subpages/ServeThePublic/public_document.aspx)  English: [TWCERT/CC Disclosure Policy](https://twcert-official-file.s3.hicloud.net.tw/CNA/TWCERTCC_Vulnerability_Disclosure_Policy.pdf) [TWCERT/CC Advisories](https://twcert.org.tw/subpages/ServeThePublic/public_document.aspx?lang=en-US) | National and Industry CERTs |
|  |  |  |  |
| VMware | VMware issues only | [security@vmware.com](mailto:security@vmware.com) | Vendors and Projects |
|  |  |  |  |
| Yandex N.V. | Yandex issues only | [browser-security@yandex-team.ru](mailto:browser-security@yandex-team.ru) | Vendors and Projects |
|  |  |  |  |
| Zephyr Project | Zephyr project components, and vulnerabilities that are not in another CNA’s scope | [vulnerabilities@zephyrproject.org](mailto:vulnerabilities@zephyrproject.org) | Vendors and Projects |
| Zero Day Initiative | Products and projects covered by its bug bounty programs that are not in another CNA’s scope | [zdi-disclosures@trendmicro.com](mailto:zdi-disclosures@trendmicro.com)  [ZDI contact page](https://www.zerodayinitiative.com/) | Bug Bounty Programs |
| ZTE Corporation | ZTE [products](https://www.zte.com.cn/global/products) only | [psirt@zte.com.cn](mailto:psirt@zte.com.cn) | Vendors and Projects |