Japan Computer
Emergency Response
Team Coordination Center

# JPCERT/CC Vulnerability Coordination and Disclosure Policy

**CONTENTS :**

**JPCERT/CC**
**2018.03.30**

## ■Overview

The purpose of vulnerability coordination and disclosure by JPCERT/CC is to enhance the Internet security by assisting product vendors' vulnerability handling and informing users of risks imposed by vulnerability and how to reduce these risks

Based on request, JPCERT/CC will coordinate the vulnerability handling process of any relevant product vendor(s) and other stakeholders in accordance with the "JPCERT/CC Vulnerability Coordination Policy". Although JPCERT/CC will attempt to coordinate as many reports as possible, we may decline to do so under some circumstances, in accordance with this policy.

JPCERT/CC will release an advisory on Japan Vulnerability Notes (JVN) in accordance with the "JPCERT/CC Vulnerability Disclosure Policy", after the vulnerability is addressed or at an appropriate time as determined by JPCERT/CC in coordination with the stakeholders involved in a coordination effort.

This document will state JPCERT/CC's vulnerability coordination and disclosure policies.

## ■Coordination Policy

### A) How to contact JPCERT/CC with a vulnerability report (coordination request)

Vulnerability reports should be sent to:

- vuls [at] jpcert [dot] or [dot] jp

We recommend using PGP. Our PGP key can be obtained from the following URL.

JPCERT/CC Vulnerability Coordination PGP Public Key
https://www.jpcert.or.jp/english/pgp/

After receiving a vulnerability report, JPCERT/CC will send an initial response (acknowledgement) to the reporter within 5 business days.

### B) What is necessary in a vulnerability report?

1. Reported vulnerability must meet the following definition:
   - A vulnerability is defined as a weakness in the computational logic found in software or other products, where there is at least one scenario that can exploit the vulnerability to negatively impact confidentiality, integrity or availability.

   - Report must not concern the ‘debug mode’ or ‘development mode’ of software
   - Report must not concern applications or products that are intentionally vulnerable for training purposes

2. The exact software version or model version affected (including a link to the product page)
   - Must be reproducible in the latest available version or at the very least an 'officially supported' version of the product
   - Must be on a product that is being 'actively' maintained
   - Must not concern a product where the developer has stated it “will not address security issues”
3. A simple description of how the vulnerability was discovered (including what tools were used)
4. Proof of concept (PoC) code or instructions that demonstrates how the vulnerability may be exploited
5. Description of the impact of the vulnerability or a threat model that describes an attack scenario
6. Report must concern a vulnerability that is not publicly known

Generally speaking, cross-site scripting will not be coordinated, unless significant impact can be demonstrated

When submitting a report, be sure to include any time constraints (for example, provide a date of publication or presentation at a conference if you know) that may apply.

JPCERT/CC may decide not to coordinate a vulnerability report. Reasons for not coordinating a report may include but not limited to the following:

- Products that have not been updated in over 18 months
- Determines that the impact to Japan the constituents is minimal

After analyzing the report, JPCERT/CC will communicate to the reporter whether or not the report will be coordinated by JPCERT/CC and provide reasoning behind the decision that was made.

Lastly, if you have already contacted the vendor or plan to contact the vendor about a vulnerability, include this information when submitting the report.

**C) What vulnerability reports will be given high priority?**

JPCERT/CC will give high priority in coordination to some reports to achieve its mission effectively. The following is a list of some criteria where a given report may be given a higher priority

- Vulnerability is deemed to have a wide effect on users in Japan
- Affects critical infrastructure
- Affects a large user base / number of products / multiple developers
- High impact

### D) What can JPCERT/CC do to assist reporters?

While JPCERT/CC may decline to provide coordinate resources, JPCERT/CC may provide the following assistance to a reporter who is coordinating on their own:

- Provide contact information for developers in Japan
- Attempt to contact a developer in Japan that has been unresponsive to the reporter

For details on assistance that will be provided, please contact JPCERT/CC

### E) In what cases will JPCERT/CC contact other parties besides the vendor?

JPCERT/CC will only contact the vendor with a vulnerability report. However, there are cases where JPCERT/CC may seek the assistance of trusted third-parties. These include:

- Consultation in obtaining a vendor contact
- Assistance in the technical analysis of a vulnerability that affects multiple vendors / implementation of protocols, etc.

### F) What does JPCERT/CC do when a vulnerability report cannot be resolved?

Unfortunately, not all vulnerabilities can be carried out through a coordinated disclosure. Some reasons for this (but not limited to) may be:

- Reporter and developer disagree on the vulnerability
- Developer does not respond to initial contact requests
- Developer stops responding to coordination requests

Either of the above will occur 120 days from initial developer contact and JPCERT/CC will consider the report 'closed'. While the reporter may ask JPCERT/CC to continue coordination, JPCERT/CC reserves the right to decline such requests

In such a case. JPCERT/CC may either,

- Make the vulnerability public (refer to "JPCERT/CC Vulnerability Disclosure Policy" for details on criteria for disclosure)
- Notify the reporter and JPCERT/CC will cease coordination attempts

### G) What does JPCERT/CC do when a reported vulnerability affects multiple vendors?

When a reported vulnerability requires multiple vendors to address a vulnerability simultaneously, ‘multi-party coordination’ occurs. For such reports, JPCERT/CC will contact multiple vendors simultaneously to address the vulnerability. The following is a list of typical scenarios where ‘multi-party coordination’ may occur:

- Supply chain vulnerability involving multiple developers and potentially service providers to address the vulnerability.
- Shared library vulnerability involving an upstream developer to address the vulnerability first and downstream developers to apply the fix.
- Protocol specification vulnerability involving developers with implementations of the protocol.

In any multi-party coordination scenario, the appropriate timing of notifying developers (upstream and downstream) and an appropriate timing for a disclosure will differ.
When involved in a multi-party coordination scenario, JPCERT/CC will attempt to balance the interests of all stakeholders involved on a case by cases basis during the coordination effort, leading to a coordinated disclosure.

## ■Disclosure Policy

JPCERT/CC will disclose an advisory on JVN when a vulnerability coordination is finished, typically with resolution by the vendor. In a coordinated disclosure, the vendor and reporter typically work together to provide a simultaneous public disclosure after a remediation is ready. In any disclosure, JPCERT/CC will not publish attack code or any unnecessary details that may cause attackers to gain an unfair advantage over defenders.

As a CVE Numbering Authority (CNA), JPCERT/CC will assign CVE’s to all vulnerabilities disclosed on JVN, unless assigned by another CNA.

In addition to coordinated vulnerability disclosures, technical alerts related to classes of vulnerabilities or attacks that affect a significant portion of the constituents are also published on JVN.

JPCERT/CC reserves the right to modify this policy at any time.

**Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)**
Hirose Bldg. 11F, 3-17 Kanda-nishiki-cho, Chiyoda-ku, Tokyo 101-0054, Japan
https://www.jpcert.or.jp/english/ mailto：vuls@jpcert.or.jp