6.10 Troubleshooting Coordinated Vulnerability Disclosure Table

The following table provides advice for resolving problems in various CVD scenarios. It is organized according to the roles affected and the phases in which the problem is likely to arise. Each problem identified is accompanied by a description intended to help the reader diagnose the problem. In addition to the advice found in the table below, we encourage readers to be familiar with 6.9 What to Do When Things Go Wrong for more general advice.

Did you notice something we missed in this table? We're taking suggestions.

Problem	Role(s) affected	Phase (s)	Description	Tips
Finder does not have the resources to shepherd a CVD case through to resolution	Finder Reporter	Discovery Reporting Validation and Triage Remediation Public Awareness	1. The vulnerability was found 2. The finder / reporter is unable to devote the necessary resources (time, effort, etc.) to following it through to resolution	Choosing to participate in Coordinated Vulnerability Disclosure can set into motion a protracted series of events which many finders and reporters may find exceeds their ability to sustain. The short answer is that you don't have to. Our experience is that many vendors are happy to receive reports even if the reporter disengages from the process immediately thereafter. The reporter's degree of involvement can therefore be self-regulating. We also remind our readers that Finders do not have to be reporters at all. We are unaware of any requirement for finders to report any vulnerabilities directly to the affected vendors. Finders that are genuinely indifferent to the effects of "dropping 0-day" always remain free to do so. (Although this likely impacts vendors' propensity to cooperate with them in the future.) Nonetheless going public with a vulnerability can be valid choice on the part of the finder. It's often informative if they also share their reason for doing so. For finders that want to be reporters but not manage the process, third party coordinators can sometimes offload some of the effort required.
Evidence of exploitation for an embargoed report	Reporter Vendor Coordinator	Discovery Reporting Validation and Triage Remediation	1. The vulnerability is still under embargo (i.e., the process has not reached the Public Awareness phase yet). 2. Evidence indicates that the vulnerability is being used by attackers. See 6.6 Active Exploitation	At this point, the embargo is effectively moot, and the Public Awareness phase has been entered regardless of whether the preceding phases have completed. Vendors, Coordinators, and Reporters should always be ready to immediately terminate an embargo and go public with whatever advice is available at the time that evidence of exploitation becomes known. The Vendor should accelerate their remediation development as much as possible. Even a simple Vendor acknowledgement that the problem is being worked on can help deployers adjust their response accordingly.
Unable to engage vendor contact	Reporter	Reporting	1. The reporter has made reasonable attempts through multiple channels to reach the vendor 2. The reporter has been unable to confirm that the vendor has received the report See 4.2 Reporting for tips on how to reach vendors. See also 6.1 Unable to Find Vendor Contact and 6.2 Unresponsive Vendor.	Assuming the reporter chooses to continue pursuing the issue at all, their options include: • The reporter may publish the report on their own. Hard-to-reach vendors often become less so after a vulnerability or two is made public without their involvement. • The reporter may attempt to engage a coordinator, to continue trying to reach the vendor
Vendor does not have a posted bug bounty	Reporter	Reporting	1. The reporter wishes to report a vulnerability to the vendor 2. The vendor does not have a public bug bounty 3. The reporter asks the vendor if they have a bug bounty 4. The vendor responds non-constructively See also 4.2 Reporting.	Up until a few years ago, bug bounties were rare. Today, vendors that intend to pay bounties for vulnerability reports have taken positive action to communicate this fact to finders and reporters. They will usually have clearly defined communication channels, program scopes, etc. posted in easily found locations. By extension, a vendor that has not taken such action has either chosen not to, or may be entirely novice to the practice of CVD. If they've chosen not to, they likely will just explain that when the reporter makes initial contact, and thus fail to meet the 4th item in the description. We've observed that some novice vendors react quite negatively to reporters who accompany their initial contact with what may appear to be a demand for payment. That's not to say that the finder or reporter intended their "do you have a bug bounty?" inquiry as an attempted extortion of course. Our recommendation to finders and reporters is that if payment for their services is expected, they do their best to find out whether the vendor offers a bounty program (and its scope) prior to embarking on any significant effort to find vulnerabilities. It's unlikely that a reporter will be able to cajole a vendor without an existing bounty to create one during the course of a single CVD case.

Vendor has a reputation for or history of treating reporters poorly	Reporter	Reporting	1. The reporter wishes to report a vulnerability to the vendor 2. The vendor has a history of treating reporters poorly (retaliation, threatened litigation, etc.) See 5.7 Disclosure Timing and 6.7 Relationships that Go Sideways.	Assuming the reporter chooses to continue pursuing the issue at all, their options include: • The Reporter may publish the report on their own, possibly anonymously. • The Reporter may attempt to engage a Coordinator to act as a neutral third party • The Reporter may attempt to engage a Coordinator to act as an anonymizing proxy to relay the information to the Vendor • The Reporter may take steps to report the vulnerability to the Vendor anonymously. The CERT/CC recommends that Reporters do their best to provide Vendors with an opportunity to resolve vulnerabilities prior to public disclosure. However if the Vendor's prior behavior makes that infeasible it's our opinion that there is a benefit to public awareness of the vulnerability regardless.
Vendor stops responding	Reporter	Reporting Validation and Triage Remediation Public Awareness	1. The reporter and vendor had already been in contact about the vulnerability. 2. The reporter has repeatedly attempted to communicate with the vendor. 3. The vendor has been non-responsive for at least two weeks 4. Either of the following events has occurred: a. An already-agreed embargo date has passed, or b. No embargo date was set and at least six weeks have elapsed since the vendor's last response. See also 6.3 Somebody Stops Replying.	At this point, the CERT/CC would consider the vendor to be non-responsive. Assuming the reporter chooses to continue pursuing the issue at all, their options include: • The reporter may publish the report on their own. If so, the reporter should provide a courtesy copy of the report to the vendor with a few days' lead time to give the vendor one last chance to prepare for entering the Public Awareness phase. • The reporter may attempt to engage a coordinator
Vendor explicitly declines to take action on a report	Reporter	Validation and Triage	1. The vendor has been given an opportunity to review the report 2. The vendor informs the reporter of its decision not to take any further action Assuming both conditions above have been met, the validation and triage phase has concluded, and the vendor has indicated that they will not be engaging in the remediation phase. See also 6.2 Unresponsive Vendor and 6.3 Somebody Stops Replying.	The reporter's implied obligation to the vendor coordination process is effectively terminated at this point. Assuming the reporter chooses to continue pursuing the issue at all, their options include: • The reporter may publish the report on their own. • The reporter may attempt to engage a coordinator
Vendor is unprepared for pending embargo expiration	Reporter Coordinator	Remediation	1. The Vendor is aware of the vulnerability. 2. The embargo date is approaching. 3. The Vendor communicates that it is not ready yet. See 5.7 Disclosure Timing	Reporters and Coordinators should consider the Vendor's responsiveness to date when deciding how to respond. If the Vendor is cooperative and seems to have a reasonable explanation for the delay, extending the embargo may be preferable. If the Vendor has had ample time to address the problem and does not appear to be acting in good faith toward a timely resolution, Reporters may choose to publish the vulnerability information on their own without the Vendor's participation. Alternatively, Reporters may choose to engage the services of a Coordinator to try to resolve the conflict. In no case is it necessary for the Reporter or Coordinators to wait indefinitely for a Vendor that does not appear to be making progress toward timely resolution.
A CVD case involves too many vendors or is otherwise excessively complex.	Reporter Vendor	Reporting Validation and Triage Remediation Public Awareness	1. Multiple vendors are likely to be affected by the vulnerability. 2. The reporter or Vendor(s) already involved are concerned about their ability to notify and coordinate other Vendors' response to the vulnerability. See also *Vulnerability affects downstream vendors* as well as 5.4 Multiparty CVD, 5.5 Response Pacing and Synchronization, and 5.6 Maintaining Pre-Disclosure Secrecy	Reporters and Vendors can engage the services of a third party Coordinator to assist with notifying other Vendors, coordinating response along a supply chain, resolving disputes, etc. Reporters and Vendors should consider shortening the embargo period for larger multiparty cases. The chance of embargo failure grows dramatically as more parties are added to the coordination.
Reporter stops responding	Vendor	Reporting Validation and Triage Remediation Public Awareness	1. The reporter and vendor had already been in contact about the vulnerability. 2. The vendor has repeatedly attempted to communicate with the reporter. 3. The reporter has not responded to the vendor. See also 6.3 Somebody Stops Replying.	The vendor is under no obligation to continue attempting to engage with a reporter who stops responding. The vendor should continue through the Validation and Triage, Remediation, and Public Awareness phases on their own as necessary. If the report was received in the context of a bug bounty program, the vendor should apply their bug bounty policy as appropriate.
Vulnerability becomes public prior to vendor intended date	Vendor	Reporting Validation and Triage Remediation	1. The vendor had received the report. 2. The vendor is working on it. 3. Information about the vulnerability appears in public. See 5.7 Disclosure Timing, 6.4 Intentional or Accidental Leaks, and 6.5 Independent Discovery	At this point, the embargo is effectively moot, and the Public Awareness phase is initiated regardless of whether the preceding phases have completed. Vendors, Coordinators, and Reporters should always be ready to immediately terminate an embargo and go public with whatever advice is available at the time that the vulnerability becomes known. The Vendor should accelerate their remediation development as much as possible. Even a simple Vendor acknowledgement that the problem is being worked on can help deployers adjust their response accordingly. The CERT/CC does not recommend punitive measures be taken against perceived "leakers". Vendors are of course free to choose with whom they cooperate in the future.
Vulnerability becomes public prior to vendor awareness of the vulnerability	Vendor	Reporting	1. The vendor was unaware of the vulnerability at the time it became public. See 5.7 Disclosure Timing, 6.4 Intentional or Accidental Leaks, and 6.5 Independent Discovery	The main defenses Vendors have against being surprised by public reports of vulnerabilities in their products are: • Vendors should have a mechanism for receiving vulnerability reports and a process for resolving them • Vendors should strive to maintain a reputation for cooperating with Finders and Reporters • Vendors should design, evaluate, and test their own products as extensively as they are able to.

Vendor receives report outside the scope of their reporting program	Vendor	Reporting Validation and Triage	1. The vendor operates a vulnerability disclosure program with a defined scope. 2. A report is received that falls outside of that scope.	Reports received in CVD programs don't always fall neatly within the vendor's predefined scope for their vulnerability disclosure policy. In most cases, that shouldn't matter, because: • If the report is for a vulnerability that the vendor is able to fix, the vendor should proceed with the rest of the CVD process as if it were in scope • If the report is for a vulnerability that the vendor is unable to fix (e.g., it's not in the vendor's product but in a library) the vendor may redirect the reporter to the originating vendor, or could act as a coordinator and engage the upstream vendor directly. • If the report is not for a vulnerability but represents a security incident (e.g., data leaked on an open server), the vendor can handle it as a security incident. • If the report is for a bug that is otherwise not a vulnerability, the vendor can route the report to the appropriate developers for remediation. In each of these cases, the reporter has provided useful information that is actionable by the vendor. Misdirected (out of scope) reports provide vendors an opportunity to review and revise their published documentation and policies to ensure they're communicating clearly what they do and do not expect to receive via their CVD program. Even if the report indicates that the finder or reporter went far beyond the vendor's policy, it may still be appropriate to handle the report as if it were in compliance in order to avoid causing further problems for either the vendor or the reporter. Reporters can often be redirected toward acceptable future behavior if their initial oversteps are treated as teachable moments rather than violations in need of punishment.
Vendor suspects the finder violated its policy in the process of finding a vulnerability.	Vendor	Reporting Validation and Triage Remediation	1. Vendor received report. 2. Vendor's analysis indicates that other policies were violated in the discovery process.	There are two issues at hand in this case: 1. Is there a vulnerability that the vendor needs to respond to? 2. Do the finder's actions constitute a security incident? Answering the first question in the affirmative, the vendor should proceed as normal through the remediation and public awareness phases. If the finder's actions are determined to qualify as a security incident of their own, the vendor would do well to consider the implied beneficence on the part of the reporter in providing the report to the vendor in the first place. Yes, rules may have been broken, but sometimes an *All's Well that Ends Well* response is preferable. Gently reminding the reporter of the vendor's expectations can help solidify a positive relationship between the vendor and the research community. That said, the above advice should not be construed as a recommendation that vendors acquiesce to aggression or abuse from finders or reporters.
Vendor receives second report of a vulnerability already under embargo	Vendor	Reporting Validation and Triage Remediation	1. The vendor had received a report of a vulnerability 2. The vendor received a second, seemingly independent, report of the same vulnerability See also 6.5 Independent Discovery.	Vulnerability rediscovery is known to happen. It's usually not a big deal if the Reporters are cooperating with the Vendor. Vendors should attempt to verify that the second report is in fact independent of the first, and not simply a case of the same report taking diverse paths to reach the vendor. Vendors should re-evaluate any existing embargo and consider accelerating the Remediation and Public Awareness phases in light of the apparent ease with which the vulnerability is being independently found. Vendors should ensure any relevant bug bounty policies define how this situation will be handled with respect to bounty payouts. If the second report is made in public rather than directly to the vendor, see also *Vulnerability becomes public prior to vendor intended date.*
Vulnerability affects downstream vendors	Vendor	Validation and Triage Remediation	1. Multiple vendors are likely to be affected by the vulnerability. 2. Many of these vendors are dependent on the originating vendor providing a fix before they can take action. 3. The originating vendor may or may not know exactly who those downstream vendors are or how to reach them. See also *Vulnerability affects unknown downstream vendors* and *Vulnerability affects multiple vendors with incompatible disclosure policies* below, as well as 5.4 Multiparty CVD, 5.5 Response Pacing and Synchronization, and 5.6 Maintaining Pre-Disclosure Secrecy	Questions of fairness arise if some affected vendors are given advance notice of a vulnerability while others are notified only when it reaches the Public Awareness phase. The goal should be to provide as much information as soon as possible to all affected vendors. Vendors should provide communication channels for their downstream vendors to coordinate vulnerability response when needed. Ideally these channels are established and maintained on an ongoing basis, because constructing them in an ad-hoc manner in the midst of a vulnerability case can be time consuming and error prone. Vendors may wish to provide an extended embargo period so that their downstream vendors have an opportunity to incorporate changes before entering the Public Awareness phase. This obviously works better in cases where the originating vendor knows who most of its downstream vendors are. (See *Vulnerability affects unknown downstream vendors* for additional advice when they don't.) Cases where a significant user base (in terms of size or relative importance) may be affected by the vulnerability via unknown downstream vendors' products are an argument in favor of shortened embargo periods and increased Public Awareness. Furthermore, the larger the number of involved parties, the more likely the embargo is to fail. Vendors in a supply chain may consider whether legally binding disclosure agreements are an appropriate means to limit this risk. However, it's often not feasible for all parties to be placed under such an agreement, which again argues in favor of short embargo periods. Reporters and Vendors can engage the services of a third party Coordinator to assist with notifying other Vendors, coordinating response along a supply chain, resolving disputes, etc.
Vulnerability affects unknown downstream vendors	Reporter Vendor Coordinator	Validation and Triage Remediation	1. Multiple vendors are likely to be affected by the vulnerability. 2. Many of these vendors are dependent on the originating vendor providing a fix before they can take action. 3. The originating vendor does not know exactly who those downstream vendors are or how to reach them. See also *Vulnerability affects downstream vendors* above, 5.4 Multiparty CVD, 5.5 Response Pacing and Synchronization, and 5.6 Maintaining Pre-Disclosure Secrecy	Questions of fairness arise if some affected vendors are given advance notice of a vulnerability while others are notified only when it reaches the Public Awareness phase. The goal should be to provide as much information as soon as possible to all affected vendors. Vendors should provide communication channels for their downstream vendors to coordinate vulnerability response when needed. Ideally these channels are established and maintained on an ongoing basis, because constructing them in an ad-hoc manner in the midst of a vulnerability case can be time consuming and error prone. For vulnerabilities affecting a large number of unknown downstream vendors, the Public Awareness phase plays an important part in identifying those vendors. Although publication may catch those by surprise in this case, it should also help establish the aforementioned contact channel for future cases. Reporters and Vendors can engage the services of a third party Coordinator to assist with notifying other Vendors, coordinating response along a supply chain, resolving disputes, etc.

Vulnerability affects multiple vendors with incompatible disclosure policies	Reporter Vendor Coordinator	Reporting Validation and Triage Remediation	1. Multiple vendors are likely to be affected by the vulnerability. 2. At least one of those vendors has a policy or practice of disclosing vulnerabilities more quickly than others. 3. That vendor is unwilling to adjust their behavior to accommodate slower vendors. See also *Vulnerability affects downstream vendors*, 5.4 Multiparty CVD, 5.5 Response Pacing and Synchronization, and 5.6 Maintaining Pre-Disclosure Secrecy	The coordinating parties (Reporter, Vendor(s), and/or Coordinator) have three options: • Shorten their embargo to accommodate the fast-moving vendor • Delay notifying the the fast-moving vendor until the other vendors are close enough that they'll be ready for the Public Awareness phase at the same time as the fast-moving vendor • Avoid notifying the fast-moving vendor during the embargo period, letting them catch up once the vulnerability enters the Public Awareness phase. The third is nearly always the least optimal of the three choices.
Vendor is unprepared for pending embargo expiration	Vendor	Remediation	1. The Vendor is aware of the vulnerability. 2. The embargo date is approaching. 3. The Vendor is not ready yet. See 5.7 Disclosure Timing	If the Vendor is working toward a solution but needs more time to complete its analysis, development, or testing, it can request an extension of the embargo from the Reporter and/or Coordinator (if any). Vendors should recognize that (absent any binding agreement to the contrary) the embargo is a courtesy offered by the Reporter or Coordinator to the Vendor, but that Reporter or Coordinator policy or other considerations may supersede the Vendor's desire for more time.
A vulnerability is receiving unanticipated media attention	Vendor	Public Awareness	1. The vendor is aware of the vulnerability, and may have already released a fix. 2. There is considerable media attention drawn to the vulnerability. a. Sometimes this is triggered by savvy marketing on the part of the Finder or Reporter b. Other times this attention comes about because of recent similar media stories. c. Often the media attention is disproportionate to the severity of the vulnerability. See also 6.8 Hype, Marketing, and Unwanted Attention	Vendors and Coordinators (if any are involved) can often help their users, constituents, and the media to appropriately calibrate their concern about a vulnerability by providing a clear and accurate representation of the facts. Vendors should not attempt to squash the information already available in the public sphere however. This often backfires, leading to even more publicity. It's better to let the vulnerability be the story rather than have the Vendor's response to the vulnerability become the story.
A CVD case just isn't going well	Reporter Vendor Coordinator	Reporting Validation and Triage Remediation Public Awareness	1. Cooperation has failed or is in the process of failing within the context of a particular CVD case. See also 6.7 Relationships that Go Sideways	All parties in a failing CVD case should consider their actions in light of promoting continued cooperation. Reporters and Vendors can engage the services of a third party Coordinator to assist with notifying other Vendors, coordinating response along a supply chain, resolving disputes, etc.