Requesting Coordination Assistance

What is Coordination?

Coordination is the process by which multiple parties coordinate to share information regarding a vulnerability, with the goal of producing a patch which fixes the vulnerability. Usually, the patch is accompanied by a security advisory, which provides the public with information on the vulnerability and how to apply the patch. However, in some cases, the security advisory may be released before a patch is available. The CERT/CC's security advisories are known as *Vulnerability Notes*.

The CERT/CC coordinates vulnerabilities with vendors, as well as provides assistance to vulnerability reporters wishing to begin the coordination process for their own vulnerability.

How Do I Begin Coordinating?

Coordinating directly with the software vendor or maintainer

We usually recommend that a reporter first try reporting the vulnerability directly to the vendor or maintainer of the software in question.

The vendor or maintainer of the software is often easy to contact and responsive to security concerns. Simply send your report to the vendor and ask what timeline for a fix is needed.

The following is a non-exhaustive list of resources that overview the coordination process, and might help a reporter find the appropriate contact at a company. The CERT/CC has not vetted any of these resources for accuracy or coverage, and only provides links for informational purposes.

- https://hackerone.com/directory
- http://disclosure.io/
- http://responsibledisclosure.nl/en/#

The EFF provides some legal guidance on the vulnerability disclosure process: https://www.eff.org/issues/coders/vulnerability-reporting-faq

However, there are several reasons for not communicating directly with the vendor. In these cases, the CERT/CC is available for assistance.

Coordinating with the CERT/CC

If any of the following conditions are true, you might consider reaching out to the CERT/CC for assistance in coordinating or publishing your case:

- if the vendor or maintainer does not reply in a reasonable time frame (typically about two weeks)
- if the vendor was initially responsive, but then stopped responding (typically about two weeks of silence)
- if the vendor has fixed a critical issue, but did not clearly document the fix in a security advisory, news article, or changelog
- if the vulnerability affects multiple vendors and would be difficult for an individual reporter to coordinate alone
- if the vulnerability is extremely serious and could cause extensive nation-wide or world-wide damage (for example, problems with internet infrastructure protocols like DNS and NTP)
- if you wish to remain anonymous (if so, you may also wish to use a pseudonym and contact CERT/CC with a free "throw-away" email account)

To request assistance, please fill out our Vulnerability Reporting Form (VRF) after reviewing our Guidelines for Requesting Coordination Assistance.

For more information about working with the CERT/CC, you may wish to read the following resources that describe our typical process:

- CERT/CC Disclosure Policy – we typically disclose vulnerability information in a publication within 45 days of initial vendor contact attempt
- Guidelines for Requesting Coordination Assistance - some tips for submitting a coordination assistance request to CERT/CC
- Understanding the Coordination Process – an overview of the typical coordination process