Working with the CERT/CC

Responding to a CERT/CC Vulnerability Notification

Be Familiar With Disclosure Policy

You may want to review our Vulnerability Disclosure Policy. In brief, we generally target publication of details of the vulnerability we reported to you 45 days after our initial contact attempt. Since our goal is a safe internet for users, we do allow some negotiation on the timeline; feel free to contact us and discuss your concerns. Likewise, we may disclose earlier than initially reported if we believe there is significant evidence of current exploit of this vulnerability.

Responding to the CERT/CC

After reviewing the vulnerability report submitted, you can respond by sending an email to cert@cert.org. When doing so, be sure to include your VU# in the subject line, so that our automated system can route your response to the analyst handling your case. If you forget to add the VU# to the subject line of your response email, our response may be delayed significantly.

We recommend encrypting your response email to cert@cert.org with the CERT/CC's PGP public key, in order to maintain privacy until the public disclosure date. For more information on using PGP or obtaining the CERT/CC's PGP key, please see Sending Sensitive Information.

To fully communicate with the CERT/CC in a secure manner, we need your organization's most up-to-date contact information, including your own PGP public key. To update your information with us, please see Updating Vendor Contact Information.

What does the CERT/CC look for in a response?

Typically, we would like the following questions answered in your organization's response:

- Is this report indicative of a real vulnerability? If not, can you provide details why you do not believe it is a vulnerability?
- Has this vulnerability already been addressed in a recent or upcoming release?
- If the vulnerability has not been addressed yet, when might the fix be available?
- Do you need any further information from the CERT/CC or the reporter in order to address this issue?

If you require extra information from the CERT/CC before a determination can be made, please feel free to contact us. The best way to do so is to send an email to cert@cert.org with your VU# in the subject line, asking for more information. You may also call our phone number during business hours and an analyst will follow up with your message.

We may also be able to arrange conference calls with analysts, or use other communication methods if requested.

Publications and Vulnerability Disclosure

After 45 days or another agreed upon timeline, we publish Vulnerability Notes on our website http://www.kb.cert.org/vuls/ to disclose the vulnerability and information on addressing the vulnerability if available.

We welcome Vendor Statements on any Vulnerability Note, even if the Note is already published. The Vendor Statement can consist of any statement or information you wish; we will copy this statement verbatim into our published Vulnerability Note. To send a Vendor Statement, please email us at cert@cert.org with the VU# of the vulnerability in the subject line, and include you statement in the body of the email. This email should be PGP signed by your organization's key so we may verify its authenticity.

Coordinating with Other Vendors

If you discover a vulnerability that might affect more products than just your own (for example, you find a vulnerability in a widely-used open source library), please feel free to reach out to us to coordinate with all vendors at once.

We can keep your organization anonymous when coordinating with other vendors.