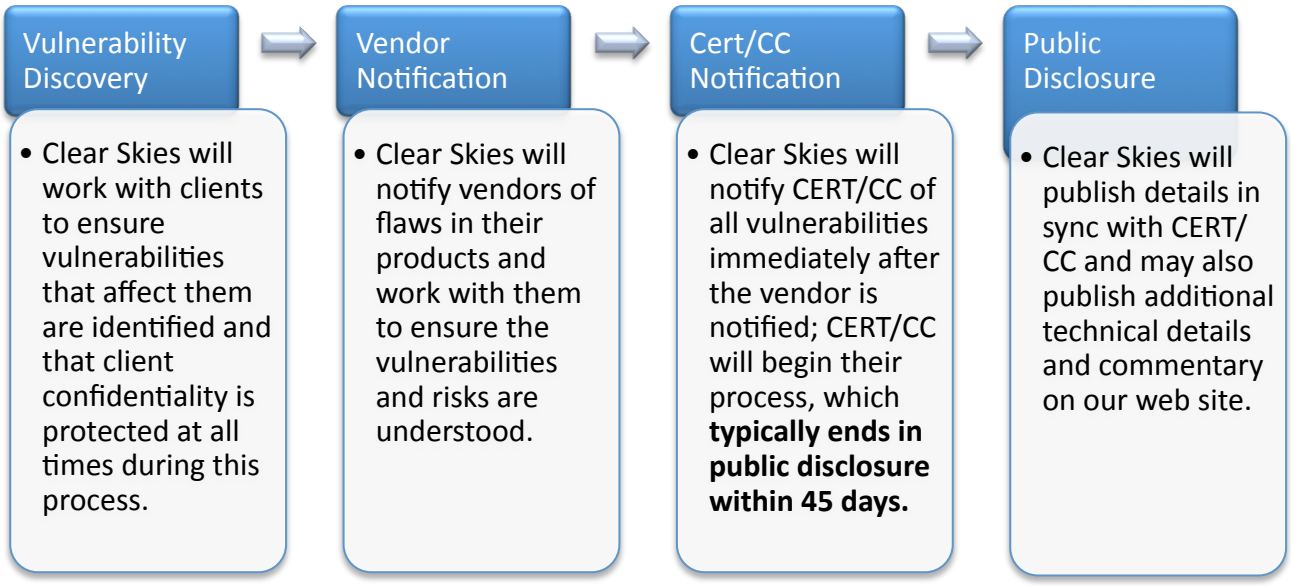
Vulnerability Disclosure Policy

April 12, 2010

SUMMARY

This document details Clear Skies Security's responsible Vulnerability Disclosure Policy, which aims to ensure that security vulnerabilities are corrected as efficiently as possible and those affected are made aware of potential risks in a reasonable timeframe.



VULNERABILITY DISCOVERY & CLIENT CONFIDENTIALITY

Clear Skies Security routinely identifies vulnerabilities during both independent research and in the course of performing work for clients. During this process, every effort is made to ensure the vulnerability is valid and to determine affected versions and configurations.

Vulnerabilities identified in the course of customer engagements are initially disclosed only to that customer. Client projects are routinely covered by non-disclosure and confidentiality agreements. Clear Skies always honors our commitments and will not disclose information covered under commitments without explicit client approval.

When a vulnerability affects a product or service supplied by a vendor that is used by others, we will pursue public disclosure of the issue without revealing any details that could be linked to a client. We will coordinate with the client during this phase to ensure they are comfortable with the generic details that will be disclosed to the public.

VENDOR NOTIFICATION

Clear Skies will next responsibly and promptly notify the appropriate product vendor of a security flaw that affects their products or services.

The first attempt at contact will be through any appropriate contacts or formal mechanisms listed on the vendor Web site, or by sending an e-mail to security@ and support *@company.com* with the pertinent information about the vulnerability.

If a vendor fails to acknowledge the initial notification within five business days, Clear Skies will initiate a second formal contact by a direct telephone call to a representative for that vendor. If a vendor fails to respond after an additional five business days following the second notification, Clear Skies will continue on to CERT notification ten business days after the initial contact.

If a vendor response is received within the timeframe outlined above, Clear Skies will make every effort to work with vendors to ensure they understand the technical details and severity of a reported security flaw. While Clear Skies is happy to work with vendors during this process, under no circumstances will Clear Skies prevent disclosure or delay the vulnerability disclosure process to accommodate vendors.

CERT NOTIFICATION

Immediately after successful vendor notification, or ten days after no response from a vendor, Clear Skies will notify CERT/CC and rely on the CERT/CC vulnerability disclosure system to provide details to the appropriate channels.

In short, this means that Clear Skies will provide details of vulnerabilities directly to CERT/CC. CERT/CC will make further attempts to ensure the vendor is notified and may also disseminate information to other security organizations. **CERT/CC will then disclose details to the public 45 days after the initial report, regardless of the availability of patches or workarounds.** In exceptional cases, CERT may shorten or lengthen this waiting period; Clear Skies will make every effort to coordinate with CERT's timeline. Refer to http://www.cert.org/kb/vul_disclosure.html for full details.

PUBLIC DISCLOSURE

Clear Skies will publicly disclose details of a vulnerability in sync with CERT/CC, which is typically 45 days after CERT/CC notification. The same details provided to CERT/CC will be published on the Clear Skies web site (http://www.clearskies.net/resources.php). Additional details, proof of concept, exploitation code, and commentary may also be provided for vulnerabilities.