The CERT/CC Vulnerability Disclosure Policy

The CERT/CC Vulnerability Disclosure Policy

Effective October 9, 2000, the CERT Coordination Center will follow a new policy with respect to the disclosure of vulnerability information. All vulnerabilities reported to the CERT/CC will be disclosed to the public 45 days after the initial report, regardless of the existence or availability of patches or workarounds from affected vendors. Extenuating circumstances, such as active exploitation, threats of an especially serious (or trivial) nature, or situations that require changes to an established standard may result in earlier or later disclosure. Disclosures made by the CERT/CC will include credit to the reporter unless otherwise requested by the reporter. We will apprise any affected vendors of our publication plans, and negotiate alternate publication schedules with the affected vendors when required.

It is the goal of this policy to balance the need of the public to be informed of security vulnerabilities with the vendors' need for time to respond effectively. The final determination of a publication schedule will be based on the best interests of the community overall.

Vulnerabilities reported to us will be forwarded to the affected vendors as soon as practical after we receive the report. The name and contact information of the reporter will be forwarded to the affected vendors unless otherwise requested by the reporter. We will advise the reporter of significant changes in the status of any vulnerability he or she reported to the extent possible without revealing information provided to us in confidence.

We anticipate the first information released under this policy to be available on or about November 20, 2000.

Vulnerabilities that are especially serious will continue to be disclosed in CERT advisories. Other vulnerabilities will be disclosed in CERT vulnerability notes. Both publications are available on the CERT web site. Additionally, CERT advisories are mailed to the CERT mailing list. For subscription information, please see http://www.cert.org/contact_cert/certmaillist.html.

Below are frequently asked questions regarding this new policy.

Q: Does this mean CERT/CC is going "full disclosure?"

A: We will not distribute exploits, if that's what "full disclosure" means. In our experience, the number of people who can benefit from the availability of exploits is small compared to the number of people who get harmed by people who use exploits maliciously. We will, however, disclose information about vulnerabilities that we might not have previously disclosed. Within the limits of our resources, we will publish information about as many vulnerabilities as we can.

Q: Why not 30 days, or 15 days, or immediately?

A: We think that 45 days can be a pretty tough deadline for a large organization to meet. Making it shorter won't realistically help the problem. In the absence of evidence of exploitation, gratuitously announcing vulnerabilities may not be in the best interest of public safety.

Q: Wouldn't it be better to keep vulnerabilities quiet if there isn't a fix available?

A: Vulnerabilities are routinely discovered and disclosed, frequently before vendors have had a fair opportunity to provide a fix, and disclosure often includes working exploits. In our experience, if there is not responsible, qualified disclosure of vulnerability information then researchers, programmers, system administrators, and other IT professionals who discover vulnerabilities often feel they have no choice but to make the information public in an attempt to coerce the vendors into addressing the problem.

Q: Will all vulnerabilities be disclosed within 45 days?

A: No. There may often be circumstances that will cause us to adjust our publication schedule. Threats that are especially serious or for which we have evidence of exploitation will likely cause us to shorten our release schedule. Threats that require "hard" changes (changes to standards, changes to core operating system components) will cause us to extend our publication schedule.

Q: Will you surprise vendors with announcements of vulnerabilities?

A: No. Prior to public disclosure, we'll make a good faith effort to inform vendors of our intentions.

Q: If a vendor disagrees with your assessment of a problem, will that information be available?

A: Yes. For serious problems disclosed in advisories, we'll solicit vendor feedback. For the less serious problems disclosed in vulnerability notes, vendors may ask for any reasonable information to be included. In either case, we will not withhold vendor-supplied information simply because it disagrees with our assessment of the problem.