Appendix D - Sample Vulnerability Disclosure Document

The vulnerability disclosure document is also often referred to as a "security advisory," particularly if published by the vendor.

This is an example of a vulnerability disclosure document based on CERT/CC's Vulnerability Notes format. It is not meant to be exhaustive of all scenarios.

Please modify the sections and format as necessary to better suit your needs.

Vulnerability Disclosure Document

Overview

• Brief Vulnerability Description: (try to keep it to 1-2 sentences)

Vulnerability ID

• CVE ID for this Vulnerability:
• Any other IDs (vendor tracking ID, bug tracker ID, CERT ID, etc.):

Description

• Software/Product(s) containing the vulnerability:
• Version number of vulnerable software/product:
• Product Vendor:
• Type of Vulnerability, if known: (see MITRE’s CWE site for list of common types of vulnerabilities)
• Vulnerability Description:
• How may an attacker exploit this vulnerability? (Proof of Concept):

Impact

• What is the impact of exploiting this vulnerability? (What does an attacker gain that the attacker didn’t have before?)

CVSS Score

• CVSS:3.0/AV:?/AC:?/PR:?/UI:?/S:?/C:?/I:?/A:? – 0.0 (LOW/MEDIUM/HIGH/CRITICAL)
• Provide the full CVSS vector, not only the score. If possible, provide guidance on the temporal and environmental metrics, not only the base metrics. See https://www.first.org/cvss/.

Resolution

• Version containing the fix:
• URL or contact information to obtain the fix:
• Alternately, if no fix is available, list workaround or mitigation advice below:

Reporter

This vulnerability was reported/discovered by ____________.

Author and/or Contact Info

For more information or questions, please contact:

• Name:
• Organization:
• Email:
• PGP Public Key (ASCII Armored or a URL):

Disclosure Timeline

• Date of First Vendor Contact Attempt:
• Date of Vendor Response:
• Date of Patch Release:
• Disclosure Date:

(List more dates here as necessary to document your communication attempts.)
References

(List reference URLs here: for example, vendor advisory, other disclosures, and links to advice on mitigating problems.)