

Appendix C - Sample Vulnerability Report Form

This is a vulnerability report, typically sent from a reporter to a vendor. These reports may also be shared among other third parties, by the reporter, the vendor, or a coordinator.

This is a report example based on the CERT/CC's [Vulnerability Reporting Form](#), and is not meant to be exhaustive of all possibilities.

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

Vulnerability Report

The information below should be handled as (choose one):

- TLP:RED
- TLP:AMBER
- TLP:GREEN
- TLP:WHITE

Vulnerability Information
Software/Product(s) containing the vulnerability:
Vulnerability Description:
How may an attacker exploit this vulnerability? (Proof of Concept)
What is the impact of exploiting this vulnerability? (What does an attacker gain that the attacker didn't have before?)
How did you find the vulnerability? (Be specific about tools and versions you used.)
When did you find the vulnerability?
Disclosure Plans
I have already reported this vulnerability to the following vendors and organizations:
Is this vulnerability being publicly discussed? YES/NO If yes then provide URL.
Is there evidence that this vulnerability is being actively exploited? YES/NO If yes, then provide URL/evidence.
I plan to publicly disclose this vulnerability YES/NO ...on this date: (Please include your time zone.) ...at this URL:
Reporter Contact Information
Name:
Organization:
Email:
PGP Public Key (ASCII Armored or a URL):
Telephone:
May we provide your contact information to third parties? YES/NO
Do you want to be publicly acknowledged in a disclosure? YES/NO
Additional Information

Vendor Tracking ID, CERT Tracking ID, or CVE ID if known:

Additional Comments:

[< Appendix B - Traffic Light Protocol](#) | [Appendix D – Sample Vulnerability Disclosure Document](#) >