There are no format limitations on the actual data, which allows for flexibility across products that may have unusual versioning or differing definitions, such as what a "problem type" means. The only exception to this is that references must be URLs. With or without this technical standard, the information referenced by each field is required.

Where applicable, make use of industry standards when describing vulnerabilities.

[PRODUCT]

As a general guideline, [PRODUCT] should include the vendor, developer, or project name as well as the name of the actual software or hardware in which the vulnerability exists.

[VERSION]

[VERSION] should include the version, date of release, or whatever indicator that is used by vendors, developers, or projects to differentiate between releases. [VERSION] can be described with specific version numbers, ranges of versions, or "all versions before/after" a version number or date.

[PROBLEMTYPE]

As mentioned above, [PROBLEMTYPE] can include an arbitrary summary of the problem.

[REFERENCES]

[REFERENCES] should be URLs pointing to a world-wide-web-based resource. For CSV and flat-file formats, they should be separated by a space. References should point to content that is relevant to the vulnerability and include at least all the details included in the CVE entry.

[DESCRIPTION]

The [DESCRIPTION] field is a plain language field that should describe the vulnerability with sufficient detail as to demonstrate that the vulnerability is unique. The required information listed above should be included in the [DESCRIPTION], as well as other details the author feels are relevant or necessary to show uniqueness.

Specifically, the [DESCRIPTION] field could also include:

- An explanation of an attack type using the vulnerability;
- The impact of the vulnerability;
- The software components within a software product that are affected by the vulnerability; and

- Any attack vectors that can make use of the vulnerability.

Descriptions often follow this template:

[PROBLEM TYPE] in [PRODUCT/VERSION] causes [IMPACT] when [ATTACK]

where impact and attack are arbitrary terms that should be relevant to the nature of the vulnerability.