Vulnerability Note Help

- Overview
- Vulnerability Notes Elements
    - Vulnerability Tracking ID
    - Title
    - Overview
    - Description
    - Impact
    - Solution
    - Vendor Information
    - Vendor Records
        - Vendor Status
        - Dates
        - Vendor Statement
        - References
        - CERT Addendum
    - CVSS Metrics
    - References
    - Acknowledgements
    - Other Information
        - CVE IDs
        - Date Public
        - Date First Published
        - Date Last Updated
        - Document Revision
    - Deprecated Elements

Overview

The following documentation describes common elements of a Vulnerability Note document. Not all Vulnerability Notes contain every element. Vulnerability Notes contain one or more vulnerabilities and one or more vendors.

Vulnerability Notes Elements

Vulnerability Tracking ID

We track vulnerability reports and publish Vulnerability Notes using a "Vee-You-Pound" number, e.g., VU#647177. VU# numbers often, but not always, have six digits. An individual vulnerability within a Vulnerability Note may be identified with either a CVE ID or a VU# number followed by a "dot" serial number, e.g., VU#647177.1.

Title

The title is a short description that summarizes the nature of the problem and the affected software components. While the name may include a clause describing the impact of the vulnerability, most names are focused on the nature of the defect that caused the problem to occur.

Overview

The overview is an abstract of the vulnerability that provides a summary of the problem and its impact to the reader. In a terse Vulnerability Note the Title and Overview may be similar.

Description

The vulnerability description contains one or more paragraphs of text describing the vulnerability. To a reasonable extent, this section focuses on the nature of the vulnerability, and the following section focuses on the potential consequences or impacts.

Impact

The impact section describes the benefit that an attacker might gain by exploiting the vulnerability. It also frequently includes preconditions the attacker must meet to be able to exploit the vulnerability.

Solution

The solution section contains information about how to correct the vulnerability. This guidance is usually general, while more vendor-specific information can be found in the Vendor Information section. The Solution section often includes workarounds or mitigation information in addition to the usual advice to "apply updates." Sub-headings are often used and appear roughly in order with more specific and effective advice first.

Vendor Information

This section (previously titled "Systems Affected") includes a list of vendors who may be affected by the vulnerability. Specifically, vendors listed here have been notified by the CERT/CC because we are reasonably concerned that the vendors may be affected by a vulnerability. Listed vendors may or may not be affected.

The list of vendors is sorted first by status (Affected, Not Affected, and Unknown), then by vendor records.

Vendor Records

An individual vendor element is called a Vendor Record. Vendor Records have several sub-elements. For a Vulnerability Note with multiple vulnerabilities, each vulnerability and its corresponding Vendor Status and Vendor Statement can be listed individually within a Vendor Record.

We notify vendors who we have sufficient reason to believe *may* be affected. Notification adds the vendor to the vendor list in the Vulnerability Note. Listing a vendor does not necessarily mean that the vendor is affected by the vulnerability.

Vendor Status

This element indicates in broad terms whether the vendor is responsible for any products, components, or services that we considers to be vulnerable or in some way affected by the vulnerability. In many cases, the relationship between a vendor's products and a vulnerability is more complex than a simple "Vulnerable" or "Not Vulnerable" status. More detailed information is often available in the Vendor Statement and other elements of the Vendor Record.

Vendor Status is not time-dependent, that is, status does not change once the vendor has released updated software or mitigation advice.

One significant factor we consider when determining vendor status is the extent to which vendors or users need to perform some mitigating activity. In the most common case, a affected vendors develop and release changed software (e.g., patch, upgrade, update) and users deploy the changed software.

Unknown

By default, vendors are marked as "Unknown." "Unknown" may indicate that we have notified the vendor but have not observed or processed a response. "Unknown" may also indicate that we have not contacted the vendor, possibly because we were unable to identify a security point of contact with reasonable effort.

Affected

If we have strong evidence (such as first-hand knowledge or vendor acknowledgement), we mark vendors as "Affected."

Not Affected

We accept assertions from vendors that they are "Not Affected" unless we have strong evidence to the contrary.

Dates

Notified

This is the date that we notified the vendor of the vulnerability. In some cases, this may be the date that the vendor first contacted us, or it may be the earliest date when the vendor is known to have been aware of the vulnerability (for example, if the vendor published a patch or an advisory).

Statement

This is when the vendor first provided a Vendor Statement.

Updated

This is when the vendor information was last updated.

Vendor Statement

This is the vendor's official response to our queries about the vulnerability. Vendors can provide their own statements, which we reproduce verbatim (or very rarely with minor formatting and grammar edits). While we try to resolve disagreements and misunderstandings, we accept that a vendor may disagree with us, and the Vendor Statement provides a way to convey the vendor's position.

We suggest that the vendors include relevant information about correcting the problem, such as pointers to software updates and security advisories.

We are highly confident that this information in this comes from the vendor. Statements are usually authenticated through VINCE, PGP-signed, or published by the vendor.

References

References are URLs provided by the vendor or the CERT/CC. If there are no references then this element heading will not appear.

CERT Addendum

This element is provided by the CERT/CC and may include additional information or commentary on a specific Vendor Record.

CVSS Metrics

As of the release of VINCE in May 2020, we are no longer providing Common Vulnerability Scoring System (CVSS) scores. Many older Vulnerability Notes include CVSSv2 vectors and scores. For those Vulnerability Notes, the following guidance applies.

> *CVSS metrics appear in vulnerability notes published after March 27, 2012. We score Temporal metrics using information available at the time the vulnerability note is first published. Temporal metric information may or may not be updated after initial publication. We score Environmental metrics with a broad scope, typically some approximation of the whole internet. To use CVSS effectively, it is important to calculate your own current and specific Temporal and Environmental metrics. For vulnerability notes that cover more than one vulnerability (e.g., multiple CVE IDs), the CVSS metrics will apply to the vulnerability with the highest CVSS base metric.*

Reasons for our decision to stop using CVSS can be found in *Towards Improving CVSS* and *Prioritizing Vulnerability Response: A Stakeholder-Specific Vulnerability Categorization*.

References

References are a collection of relevant URLs. We attempt to list original source material first, and sometimes include references to high quality second-hand material as well.

Acknowledgements

Unless otherwise requested, we acknowledge individuals and organizations who report vulnerabilities to us. This element identifies who reported the vulnerability, anyone who was instrumental in the development of the Vulnerability Note or assisted significantly in the coordinated vulnerability disclosure process, and the primary author of the Vulnerability Note.

Other Information

These elements provide additional information about the Vulnerability Note.

CVE IDs

CVE IDs are used to uniquely identify a vulnerability. The ID is also a link to additional information on the NIST National Vulnerability Database (NVD). In some cases, a Vulnerability Note may not include CVE IDs. The mapping between CVE IDs and VU# numbers may not be one-to-one.

Date Public

This is the date on which the vulnerability was first known to the public, to the best of our knowledge. Usually this date is when the Vulnerability Note was first published, when an exploit was first discovered, when the vendor first distributed an update publicly, or when a description of the vulnerability was made public.

Date First Published

This is the date when we first published the Vulnerability Note.

Date Last Updated

This is the date the Vulnerability Note was last updated. Since each vulnerability note is updated as we receive new information, this date may change frequently. This date is also updated when vendor information changes.

Document Revision

This number is updated when the Vulnerability Note is modified and republished.

Deprecated Elements

These elements appear in some older Vulnerability Notes.

US-CERT Alert

If a US-CERT Alert was published for this vulnerability, this field will contain a reference to the alert.

CERT Advisory

If a CERT Advisory was published for this vulnerability, this field will contain a reference to the advisory. Beginning January 28, 2004, CERT Advisories became a core component of US-CERT Alerts.

Severity Metric

Note: Vulnerability Notes published after March 27, 2012 will use CVSS metrics instead, and Vulnerability Notes published after May 2020 contain neither the Severity Metric nor CVSS metrics.

The metric value is a number between 0 and 180 that assigns an approximate severity to the vulnerability. This number considers several factors, including:

- Is information about the vulnerability widely available or known?
- Is the vulnerability being exploited?
- Is the Internet Infrastructure at risk because of this vulnerability?
- How many systems on the Internet are at risk from this vulnerability?
- What is the impact of exploiting the vulnerability?
- How easy is it to exploit the vulnerability?
- What are the preconditions required to exploit the vulnerability?

Because the questions are answered with approximate values that may differ significantly from one site to another, users should not rely too heavily on the metric for prioritizing vulnerabilities. However, it may be useful for separating the very serious vulnerabilities from the large number of less severe vulnerabilities described in the database. The questions are not all weighted equally, and the resulting score is not linear (a vulnerability with a metric of 40 is not twice as severe as one with a metric of 20).