CVE Record Management Guidelines
July 14, 2023

It is important we protect the integrity of the CVE Records. Changes made to existing CVE Records needs to be limited to changes either correcting CVE-related information or providing better vulnerability related explanations.

The following guidelines must be followed in the short term and are actively being incorporated into the CVE Program Rules. The guidelines depicted below are subject to change and are expected to be enhanced in the future.

Background

Prior to October 2016, the CVE Program was based on a hub and spoke model and MITRE was the hub. In that capacity, MITRE wrote all CVE descriptions and published all CVE Records. While there were a few CVE Numbering Authorities (CNAs) before that date, it was not until early 2017 the program began to change from its initial model to the current federated CNA management model. Today, it is CNAs responsibility to write their own descriptions and publish their own records.

The CVE Board has defined October 31, 2016, as the point in time where all CVE Records prior to that date are deemed historical CVE data.

Modification of Historical CVE Data

- CVE Records created prior to October 31, 2016, must not be modified by CNAs. This restriction will be implemented in CVE Services so that any attempt to change historical data will be blocked.

- If your organization feels there is a legitimate need to make changes to relevant records, contact the CVE Secretariat and make your case. Due to CVE Board directions, the Secretariat most likely will not accept your request. However, if there are errors that need to be corrected, contact the Secretariat with the justification and suggested updates so the supplied information can be reviewed, and records updated if deemed appropriate.

Modification to CNA CVE Data

- CVE Records created after October 31, 2016, can be updated by the owning CNA.

- CVE Descriptions are highly visible to the vulnerability management community that use CVE data in products, databases and security advisories. When updating existing CVE Descriptions, adherence to the following guidelines is required:

    a. *Additional clarifying detail*: Information that enhances understanding of the vulnerability is allowed and encouraged.
    b. *Errors*: Where a description contains an error, it should be corrected.
    c. *Removing information*: Removing information from a description that is not in error is not allowed.

d. ***Altering information:*** Changing information in a description to modify the perceived severity of a vulnerability is not allowed.

Temporary CVE Record Modification Considerations

- **Description Length:** The CVE Program is deprecating the CVE JSON 4.0 data format. The completion to only supporting CVE JSON 5.0 is planned for July 1, 2024. Until then, there is a limit on the CVE Record Description field to a maximum of 3999 characters. Be aware of this when developing descriptions. The Program is exploring an auto-truncate feature which will truncate descriptions to the maximum allowable character count of 3999. Until this feature is available, descriptions surpassing the character count will cause the submission to fail.

- **Existing External References:** CNAs **must** preserve existing references. It is possible to unintentionally overwrite existing references through an update process. This is a short-term problem being addressed through the CVE Program ADP container when operational in the coming months. At that point existing references will be copied from the CNA container from all CVE Records into the CVE Program ADP container. However, until this capability is operational, CNAs must pay close attention to not accidentally overwrite existing references during an update process:
  a. All references (initial and added) must be retained during any updates.
  b. Broken historical links must be retained for historical reference.
  c. When references added by the CNA are not correct (e.g., due to input errors, M&A activities, etc.) corrections are allowed.

Questions

If you have any comments or concerns, please use the CVE Program Request forms and select "Other" from the dropdown menu.