End of Life Vulnerability Assignment Process

August 3, 2020

Version 1.1

Approved by CVE Board on July 7, 2020

Table of Contents

1 Introduction

The mission of the CVE Program is to identify and define publicly disclosed security vulnerabilities for consumption by the computing community. Significant debate has occurred within the CVE Program regarding whether CVE Records should be assigned for End-of-Life (EOL) products. This document is the result of those conversations. The purpose of this document is to establish a policy and detail a process by which the equities of all program participants can be aligned, consistent with the CVE Program's mission.

2 Background

A Vendor CVE Numbering Authority (CNA) assigns CVE IDs and publishes CVE Records for products within their distinct, agreed upon program scope. Many Vendor CNAs treat CVE IDs as part of product vulnerability response and remediation processes, i.e., CVE IDs are assigned as product vulnerability fixes are published. Vendors do not typically produce fixes for products that they no longer support. Vendor CNAs may choose not to investigate or attempt to reproduce vulnerabilities reported in EOL products. Such an investigation may be cost-prohibitive, if not impossible. Vendor CNAs can declare that products listed in a CVE Record are EOL and take no further action. The CVE Program facilitates this declaration through the use of the CVE EOL tag and educational documentation on the CVE website.

There has been an ongoing, robust discussion within the CVE Program as to whether or not EOL products should be assigned CVE IDs.

Vendor CNAs contend that it is unnecessarily costly for them to deal with vulnerability inquiries regarding EOL products, especially if it requires them to spin up teams to validate a reported vulnerability in an EOL product customers should not be running. The problem is, to verify that a vulnerability exists, the vendor would have to test and validate it. Many vendors do not see any value in spending time, effort and resources on a discontinued product that should be removed from operational use. Vendors would prefer customers upgrade to newer versions of the product which are supported, rather than continue using outdated and officially unsupported EOL products.

Other CVE Program participants, however, believe vulnerabilities in EOL products should be assigned because the vulnerabilities exist and users of EOL products should have knowledge of how they are vulnerable, regardless of the efficacy of using EOL products.

Since legitimate vulnerabilities are sometimes discovered in EOL products still being fielded, it is necessary for the CVE Program to have a documented and transparent process for dealing with these types of reported EOL vulnerabilities.

While there has not been unanimous consensus among the CVE Board members or the CNAs themselves, there was agreement that the mission of the CVE Program is to identify, catalog, and assign IDs to publicly known security vulnerabilities and that CVE IDs may be assigned for EOL product vulnerabilities that meet the requirements outlined in the CVE assignment rules (which are listed in the CNA Rules).

3 Temporary CNA Rules Inconsistency

The CNA Rules v3.0, effective March 5, 2020, states:

"A CNA should list in their scope whether they want to handle CVE assignments for end-of-life components according to the end-of-life rules or whether other CNAs should assume that responsibility if they have a need to reference such vulnerabilities. If a CNA specifies that it will not assign for end-of-life components, other CNAs may assign for those components."

It should be noted that this is not required to be incorporated into the CNA's scope statement at this time.

The CNA Rules for EOL must be re-addressed, as the wording of the current rules conflict with the agreed to process for handling EOL vulnerability reports. Below is suggested wording to correct the existing shortcomings:

"A CNA may list, in its scope, whether it does or does not want to handle CVE assignments for end-of-life components or products. If a CNA does not specify end-of-life handling in its scope, then all EOL vulnerabilities should be reported through the CNA's official processes. If a CNA specifies that it will not assign for end-of-life components, then the documented applicable CVE EOL process should be followed. Top Level Roots (TLR) will define how the EOL process is to be used within their hierarchy."

4 CVE Program Principles

The following is a list of fundamental principles that should be understood by all parties participating in the CVE Program, including CNAs, vulnerability reporters, and CVE consumers:

- CVE IDs may be assigned for vulnerabilities in EOL products.
- There are no expectations of vendors to either investigate or correct vulnerabilities reported in EOL products.
- Vendor CNAs have the first "right-of-refusal" in issuing CVE IDs for their products, but cannot stop the assignment of a CVE ID if deemed appropriate by the program.
- If a Vendor CNA does not assign, the CNA of Last Resort (CNA-LR) will work with both parties (Vendor CNA and the Reporter) to determine whether or not to assign a CVE ID to a vulnerability in an EOL product.
- CVE IDs assigned for EOL products are to be tagged with a ***Unsupported When Assigned*** tag.

5 CVE Program EOL Assignment Process

The following section documents the CVE Program's Default EOL Assignment process.

When a reporter believes they have found a vulnerability in an EOL product, they must follow the process below to have a CVE ID assigned to it:

1. **The Reporter locates the appropriate CNA's contact and scope information.**

   CNA contact information can be found in the participating CNA section of the CVE website. If the documented Vendor CNA scope states they are supporting EOL assignments, or does not specify, the Reporter must contact the appropriate Vendor CNA using the published official contact information. If the scope states the Vendor CNA does not support issuing CVE IDs for its EOL products, the Reporter will not need to contact the Vendor CNA and instead should contact the appropriate CNA-LR for the hierarchy.

2. **Reporter contacts the Vendor CNA**

   When the Reporter contacts the Vendor CNA regarding a vulnerability in an EOL product, the Reporter is required to provide some means of depicting how the issue was discovered and proof of the vulnerability's existence to the Vendor CNA. It is up to the Vendor CNA to make the decision as to how to proceed. Depending on the product and circumstances, the Vendor CNA decides whether or not to assign a CVE ID for the discovered issue. If they do assign a CVE ID, the process is complete.

3. **Vendor decides not to assign**

   If the Vendor CNA decides not to assign a CVE ID, the Vendor CNA must notify the Reporter of their decision and provide a reason why the decision was made not to assign. In such cases where the Vendor CNA chooses not to assign CVE IDs and publish CVE Records for EOL products, the product falls out of the Vendor CNA's scope for the purpose of CVE ID assignment and CVE Record publication. If the Reporter believes there is a need for this vulnerability to have a CVE ID assigned, the Reporter can then escalate the request to the CNA-LR to request the CVE ID. In these cases, the CNA-LR is empowered to assign and publish if deemed appropriate.

4. **The Reporter escalates the issue to the CNA-LR at the same hierarchy level**

   When the Reporter contacts the CNA-LR regarding a vulnerability in an EOL product, the Reporter is required to provide some means of depicting how the issue was discovered and proof of the vulnerability's existence to the CNA-LR.

5. **CNA-LR verifies the Reporter has contacted the Vendor CNA**

   Before a CNA-LR can take up the issue, and providing the Vendor CNA's scope does not preclude assigning for EOL products, the CNA-LR must verify the Reporter has contacted the Vendor CNA. If they have not, the CNA-LR instructs the Reporter to do so before the CNA-LR can proceed. The CNA-LR will request the email thread that included the Vendor CNA's response and their reasons for declining the initial request for a CVE ID.

6. **CNA-LR confirms the Vendor CNA is not going to assign**

   If the Vendor CNA's scope does not preclude assigning for EOL products, the CNA-LR must contact the Vendor CNA to ensure the CNA-LR has a true picture of the situation. Initial contacts must go through official channels; however, alternate contacts may be used if initial contacts prove unresponsive. The response must come from an authorized point of contact, through the CNA's official channel. If the Vendor CNA has decided to assign a CVE ID, the CNA-LR will redirect the Reporter back to the Vendor CNA and

the CNA-LR's role is complete. If the CNA is not responsive in a reasonable timeframe, the CNA-LR should proceed with the process documented below.

7. **Determining the validity**

   If the CNA-LR confirms that the Vendor CNA is not going to assign, either by specified scope or by communication with the Vendor CNA, the CNA-LR needs to determine whether there is a valid reason a CVE ID should be assigned. There can be valid reasons for a CVE-ID not to be assigned. Before the decision can be made, the CNA-LR needs to obtain as much information about the issue as possible. The CNA-LR, as appropriate, needs to take both the Vendor CNA's, and the Reporter's reasoning into account and give each an opportunity to respond to the other's reasoning. The CNA-LR will use the information supplied by both parties in determining if a CVE ID should be assigned for an unvalidated vulnerability. The CNA-LR will use the information supplied by both parties in making its decision.

8. **The CNA-LR's Assignment Decision**

   The CNA-LR determines if there is a need for an assignment. The CNA-LR must apply the assignment rules. However, in these situations, 7.1.3[1] must not be used when determining whether the issue should be considered a vulnerability. If the CNA-LR determines there is a need for a CVE ID to be assigned, then the CNA-LR will assign the CVE ID, and publish the CVE Record with the appropriate information. The CVE Record must include the ***Unsupported When Assigned*** tag.

9. **Vendor CNA Notification**

   The CNA-LR will notify the Vendor CNA and the Reporter of what decision was made, why it was made, and what actions were taken based on the decision.

6 EOL CVE ID Tagging

The ***Unsupported When Assigned*** tag (i.e., End-of-Life or EOL tag) is added to the description by the assigning CNA to indicate that when a request for a CVE ID was received, the product was already EOL. It indicates the CVE Record tagged with an EOL tag was requested and assigned after a product or specific product line was deemed not to be supported by the vendor. The vendor is under no obligation or responsibility to test, validate, or fix a vulnerability found in a product that is no longer supported by the vendor. For the CVE Program's purposes, the EOL status for a product or version line is when it will no longer receive security fixes, regardless of what term the maintainer uses to designate this status. Users are encouraged to upgrade to a supported version (if there is one), replacing the product, or implement some other mitigation.

[1] CNA Rules v3.0, 7.1.3 states, "If a CNA receives a report about a new vulnerability that has a negative impact, then the reported vulnerability MAY be considered a vulnerability."

6.1 Tagging Use and Considerations

While the ***Unsupported When Assigned*** tag describes the product ID (not the CVE ID), it is applied to the CVE ID due to the manner in which CVE ID assignments are made. The ***Unsupported When Assigned*** tag should only be applied to a CVE Record when all affected products or version lines referenced in the CVE ID are EOL. If some of the affected products or versions have reached EOL but others have not, then the tag must not be used. If the CVE Record has both non-EOL and EOL products, the maintainers are not required to list the EOL products in the CVE Record.

CVE Records that existed prior to the product becoming EOL will not be marked with the ***Unsupported When Assigned*** tag when the product transitions to EOL. The purpose of the tag is to notify the community that a vulnerability report was received when the product was already EOL and the Vendor has no responsibility to validate or fix the reported issue.

The data publisher (Vendor CNA or CNA-LR) must provide a reference to the CNA-specific EOL information, which typically informs customers how to upgrade to a currently supported product.

Regardless of who assigns an EOL CVE ID, it is important to ensure the record is tagged appropriately. An EOL tag is included in the description which is beneficial for the downstream uses and consumers of CVE. Additionally, an EOL tag is indicated in the CVE Record tag attribute in order to facilitate filtering and metrics.

6.2 What an Unsupported When Assigned CVE Record Looks Like

** UNSUPPORTED WHEN ASSIGNED ** [VULN INFO HERE] NOTE: This vulnerability only affects products that are no longer supported by the maintainer.

6.3 JSON Schema unsupported-when-assigned Attribute Tag

A “tags” property is a part of the CNA and ADP containers in the JSON schema. The value of this property will be an array of string values. The “*unsupported-when-assigned*” tag will be used when appropriate as documented above.

For example:

```
{
   "data_format": "MITRE",
   "data_type": "CVE",
   "data_version": "5.0",
   "CVE_data_meta": {
      "ASSIGNER": "cve@mitre.org",
      "ID": "CVE-YYYY-NNNNN",
      "STATE": "PUBLIC",
      "DATE_ASSIGNED":"2019-01-01 23:45:00+0500",
```

```
    "DATE_PUBLIC":"2019-12-13 08:45:00+0500"
  },
  "containers": {
    "CNA": {
      "provider_data_meta": {
        "ID": "cve@mitre.org",
        "UPDATED": "2019-01-01T23:45:00Z"
      },
      "descriptions": [
        {
          "lang": "EN",
          "value": "ACME Spy Be Gone 6.6 below have Incorrect Access Control."
        }
      ],
      "tags": [ "exclusively-hosted-service", "unsupported-when-assigned" ]
    },
    "ADPs": [
      {
        "provider_data_meta": {
          "ID": "user@example.com",
          "UPDATED": "2019-01-01T23:45:00Z"
        },
        "description": [
          {
            "lang": "FR",
            "value": "ACME Spy Be Gone 6.6 ci-dessous a un contrôle d'accès incorrect."
          }
        ],
        "tags": [ "other-tag-1" ]
      }
    ]
```

```
   }
}
```

The *unsupported-when-assigned* tag is only allowed to be used in the CNA container. For EOL tagging, this ensures that the CNA making the CVE ID assignment and publishing the CVE Record is clearly identified.

7 Controlling the Messaging

CNAs have expressed concern that the EOL process takes the assignment of certain vulnerabilities out of their hands. They contend that since the affected EOL products are their products, the CVE Program should not allow assignments for possible vulnerabilities that are not verifiable. Vendor CNAs who have been reluctant to assign CVE IDs for EOL products may want to reconsider. While it can be difficult to prove there is a vulnerability, using the EOL process to make assignments gives the Vendor CNA an opportunity to communicate, to the community and their customers, that the product is EOL and gives them another vehicle for reaching those who need to be aware they should upgrade their fielded products. An example of a possible message template is included below.

> *** UNSUPPORTED WHEN ASSIGNED ** [VULN INFO HERE] We cannot prove this vulnerability exists. Out of an abundance of caution, this CVE ID is being assigned to better serve our customers and ensure all who are still running this product understand that the product is end of life and should be removed or upgraded. For more information on this, and how to upgrade, refer to the CVE Record's reference information.*

Using this approach, a vendor could justify assigning CVE IDs for all reported EOL vulnerabilities, thus modeling proactive, customer-focused behavior. Externally, the company looks proactive and customer focused. If the CVE ID assigned to an EOL product is later discovered in a vulnerability scan, the description will reinforce that the product is no longer supported, and the customer may need to take action. This approach also has the potential to discourage the unethical practice of someone hunting for vulnerabilities in EOL products for the purpose of boosting their professional reputation.

8 CVE Program EOL Process Benefits

The EOL process outlined in this document serves all CVE Program stakeholders to the degree possible (i.e., vulnerabilities are not hidden, but consumers are made aware they should not expect any mitigations or patches). The CVE EOL process provides another mechanism for Vendor CNAs to communicate to customers that EOL products are not supported and customers should upgrade to the latest version. And finally, the process is consistent with the CVE Program's mission to assign CVE IDs and publish CVE Records for publicly known vulnerabilities.

Appendix A Definitions

CVE Participants: Anyone who is an active participant in the CVE Program, including CVE Board members, CNAs, Authorized Data Publishers (ADPs), and the CVE Program Secretariat.

CNA-LR: The CNA-LR function must exist within each TLR hierarchy. Within that hierarchy, the CNA-LR function assigns CVE IDs and publishes CVE Records not covered by another CNA's distinct, agreed upon scope.

EOL: For the purpose of this document, End of Life (EOL) and End of Support (EOS) are being treated as the same, even though various vendors may use these terms differently. EOL essentially means the vendor has decided the product in question has reached the end of its "useful lifespan." After this particular date, the manufacturer no longer markets, sells, provides technical support, sustains, enhances, or fixes the product.

Reporter: The Reporter is the person that discovers and reports the vulnerability. It could be a security researcher, a corporate partner, an end-user, etc.

Top Level Root (TLR): The highest level Root of a specific CNA hierarchy.

Vendor: A vendor is anyone that creates, distributes, and maintains products, regardless of whether the product is an open source project deliverable or a commercial product.