CVE Program Policy for End of EOL Products

This policy is Section 5 within the larger "End of Life Vulnerability Assignment Process" document.

When a reporter believes they have found a vulnerability in an "End of Life (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. [2]

[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."

[2] See Section 6 of the End of Life Vulnerability Assignment Process for more information on tagging.