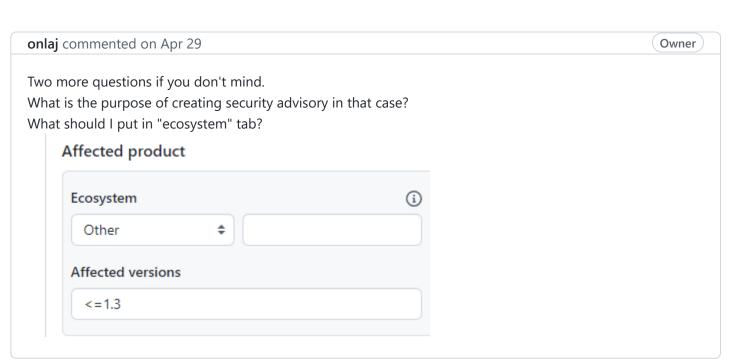


Sure, I can do it. Should I copy into the description what you wrote in the #350?





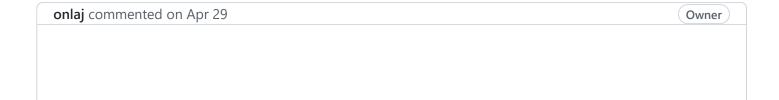


@onlaj Ecosystem means the primary language ecosystem to which the project belongs. In this case, since the bug is in python code, you may select <code>pip</code>.

As for severity, please select assess severity using CVSS. Then please paste the following CVSS vector in the input.

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:L

For CWE, please put CWE-073. In the CVE field, select request CVE ID later. Github will go through the submission and issue a CVE. You can use this CVE ID to notify downstream users of the vulnerability and the fix.



I made a draft and added you as collaborator, but I still don't fully understand what is it for.

I can press "Request CVE" and it says that: Once requested, GitHub will review this advisory in order to assign a CVE.

If I understand it correctly they will use it to notify other users about that vulnerability if it is found in their repositories, right?

porcupineyhairs commented on Apr 29

Contributor

Author

@onlaj I have made a bunch to the draft advisory. PTAL.

A CVE ID is used to identify a security vulnerability in a product. By issuing a CVE you allow the users of your software to be notified about a security vulnerability. If this software is used by other downstream libraries, a CVE would nudge them to upgrade to the patched version. Also sometimes, Github may even create a dependabot alert for users to auto-patch the bug.

onlaj commented on Apr 29

Owner

Ok, I understand now.

Should I "Request CVE" or "Publish advisory"?

porcupineyhairs commented on Apr 29

Contributor

Author

@onlaj I don't know. You should be doing both. I think request CVE would automatically publish the advisory so try that.

া onlaj merged commit 3f10602 into onlaj:master on Apr 29

porcupineyhairs mentioned this pull request on May 4

Python: Flask Path Traversal Vulnerability github/securitylab#669

Closed

2 tasks

scaraude pushed a commit to scaraude/Piano-LED-Visualizer that referenced this pull request on Jun 6

Merge pull request onlaj#351 from porcupineyhairs/FixPathInjection ...

51c17c6

No reviews
Assignees
No one assigned
Labels
None yet
Projects
None yet
Milestone
No milestone
Development
Successfully merging this pull request may close these issues.
Security Vulnerability Found
2 participants