OPNFV Security Vulnerability Management (OSVM)

Advisory Database

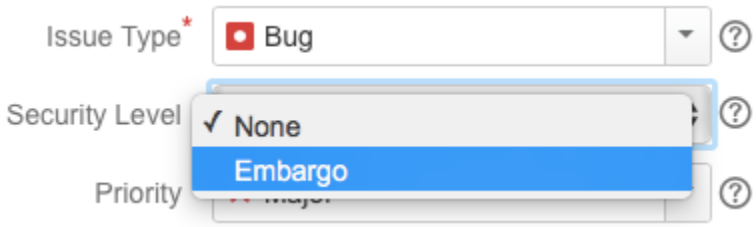
A database is maintained of previous reported advisories can be found here: Previous OSVM Advisory's

How to report vulnerabilities in OPNFV projects.

Security vulnerabilities should be reported through the relevant project JIRA, by setting the security level to "Embargo" when creating an issue. Before reporting a Security Vulnerability in JIRA, please make sure that the project is a vulnerability managed project. You can tell that a project is a vulnerability managed project if you see the "Security Level" field when you click "Create" and select the relevant project (see image below).

If the project is not a vulnerability managed project, as described above, please contact the project PTL and/or the OPNFV TSC and request this capability (see below). In your request, note that you are attempting to report a security vulnerability and, therefore, the request is urgent.

Additional details about completing a security vulnerability report in JIRA may be found here.



Initial response time

OPNFV project's goal for initial response time for vulnerability response is less than **7 working days**. This is however not a guarantee but a goal set by the team. Under some circumstances (e.g. during vacation period of members) some variation might occur.

If you have not received a response within a week, please alert the TSC, and the associated project PTL, that you have filed a security vulnerability issue. When doing so, DO NOT include details about the vulnerability, just simply alert the TSC, and the associated project PTL, that you have reported a vulnerability.

How to become a vulnerability managed project in OPNFV.

Projects may have security vulnerabilities managed under the OSVM process, by requesting a security scheme in jira. Requests may be made to the OPNFV Help Desk. DO NOT include any details about a security vulnerability in the request.

This will then allow a project to have vulnerabilities handled under a public embargo. A JIRA issue can marked as private, allowing co-ordination with the security group, while a patch is prepared in private.

How to become a downstream stakeholder

Suppliers / Distributors of OPNFV can request allocation as a downstream stakeholder. Downstream stakeholders are notified 3 to 5 working days in advance of private issues / patches being made public. This then allows them time to plan maintenance windows / patch application processes.

To request allocation as a downstream stakeholder, please email lhinds [at] redhat [dot] com or Sona [dot] Sarmadi [at] enea [dot] com

Overview of OSVM

The OSVM process is to manage and coordinate the disclosure and management of vulnerabilities reported or discovered within the opnfv-eco system and upstream projects.

The process inherits from the already present and well functioning OSSG VMT Process and follows the Responsible Disclosure Approach

Draft OSVM Embargoed Vulnerability Management Process

The diagram below uses "@" to describe various stakeholders in the process. Note that these are NOT email addresses. Please do not use them for vulnerability reporting.