Defect Response

Reporting a Security Bug

If you think you have discovered a security issue in any of the Hyperledger projects, we'd love to hear from you. We will take all security bugs seriously and if confirmed upon investigation we will patch it within a reasonable amount of time and release a public security bulletin discussing the impact and credit the discoverer.

There are two ways to report a security bug. The easiest is to email a description of the flaw and any related information (e.g. reproduction steps, version) to security at lists dot hyperledger dot org.

For Fabric, you may use HackerOne.

Security Bug Handling Process

The process the Hyperledger Security Team will follow when dealing with security bugs is detailed below:

1. The person discovering the issue, the reporter, reports the vulnerability privately to security at lists dot hyperledger dot org
2. Messages that do not relate to the reporting or managing of an undisclosed security vulnerability in Hyperledger software are ignored and no further action is required.
3. The project team sends an e-mail to the original reporter to acknowledge the report.
4. The project team investigates report and either rejects it or accepts it.
5. If the report is rejected, the project team writes to the reporter to explain why.
6. If the report is accepted, the project team writes to the reporter to let them know it is accepted and that they are working on a fix.
7. The project team requests a CVE number from security at lists dot hyperledger.org by sending an e-mail with the subject “CVE request for…” and providing a short (one line) description of the vulnerability. Guidance is available to determine if a report requires multiple CVEs or if multiple reports should be merged under a single CVE.
8. The project team agrees the fix on their private list.
9. The project team provides the reporter with a copy of the fix and a draft vulnerability announcement for comment.
10. The project team agrees to the fix, the announcement and the release schedule with the reporter. For an example of an announcement see Tomcat's announcement of CVE-2008-2370. The level of detail to include in the report is a matter of judgement. Generally, reports should contain enough information to enable people to assess the risk associated with the vulnerability for their system and no more. Steps to reproduce the vulnerability are not normally included.
11. The project team commits the fix. No reference should be made to the commit being related to a security vulnerability.
12. The project team creates a release that includes the fix.
13. The project team announces the release. The release announcement should be sent to the usual mailing lists (typically the project's user list, dev list, announce list and the Hyperledger announce list).
14. The project team announces the vulnerability. The vulnerability announcement should be sent after the release announcement to the following destinations:

    a. the same destinations as the release announcement
    b. the vulnerability reporter
    c. the project's mailing list.
    d. https://cveform.mitre.org/ and use “Notify CVE about a publication”. Submissions should be in the following format:

```
[CVEID]:CVE-2017-5648
[PRODUCT]:Apache Tomcat
[VERSION]:9.0.0.M1 to 9.0.0.M17, 8.5.0 to 8.5.11, 8.0.0.RC1 to 8.0.41, 7.0.0 to 7.0.75
[PROBLEMTYPE]:Information Disclosure
[REFERENCES]:https://lists.apache.org/thread.html
/d0e00f2e147a9e9b13a6829133092f349b2882bf6860397368a52600@%3Cannounce.tomcat.apache.org%3E
[DESCRIPTION]:While investigating bug 60718, it was noticed that some calls to application listeners
did not use the appropriate facade object. When running an untrusted application under a
SecurityManager, it was therefore possible for that untrusted application to retain a reference to
the request or response object and thereby access and/or modify information associated with another
web application.
```

15. This is the first point that any information regarding the vulnerability is made public.

Information may be shared with domain experts (e.g. colleagues at your employer) at the discretion of the project's security team providing that it is made clear that the information is not for public disclosure and that security at lists dot hyperledger dot org must be copied on any communication regarding the vulnerability.