c-ares security

This document is intended to provide guidance on how security vulnerabilities should be handled in the c-ares project.

Publishing Information

All known and public c-ares vulnerabilities will be listed on the c-ares web site.

Security vulnerabilities should not be entered in the project's public bug tracker unless the necessary configuration is in place to limit access to the issue to only the reporter and the project's security team.

Vulnerability Handling

The typical process for handling a new security vulnerability is as follows.

No information should be made public about a vulnerability until it is formally announced at the end of this process. That means, for example that a bug tracker entry must NOT be created to track the issue since that will make the issue public and it should not be discussed on the project's public mailing list. Also messages associated with any commits should not make any reference to the security nature of the commit if done prior to the public announcement.

- The person discovering the issue, the reporter, reports the vulnerability privately to `c-ares-security@haxx.se`. That's an email alias that reaches a handful of selected and trusted people.
- Messages that do not relate to the reporting or managing of an undisclosed security vulnerability in c-ares are ignored and no further action is required.
- A person in the security team sends an e-mail to the original reporter to acknowledge the report.
- The security team investigates the report and either rejects it or accepts it.
- If the report is rejected, the team writes to the reporter to explain why.
- If the report is accepted, the team writes to the reporter to let him/her know it is accepted and that they are working on a fix.
- The security team discusses the problem, works out a fix, considers the impact of the problem and suggests a release schedule. This discussion should involve the reporter as much as possible.
- The release of the information should be "as soon as possible" and is most often synced with an upcoming release that contains the fix. If the reporter, or anyone else, thinks the next planned release is too far away then a separate earlier release for security reasons should be considered.

- Write a security advisory draft about the problem that explains what the problem is, its impact, which versions it affects, solutions or workarounds, when the release is out and make sure to credit all contributors properly.
- Request a CVE number from distros@openwall when also informing and preparing them for the upcoming public security vulnerability announcement - attach the advisory draft for information. Note that 'distros' won't accept an embargo longer than 19 days.
- Update the "security advisory" with the CVE number.
- The security team commits the fix in a private branch. The commit message should ideally contain the CVE number. This fix is usually also distributed to the 'distros' mailing list to allow them to use the fix prior to the public announcement.
- At the day of the next release, the private branch is merged into the master branch and pushed. Once pushed, the information is accessible to the public and the actual release should follow suit immediately afterwards.
- The project team creates a release that includes the fix.
- The project team announces the release and the vulnerability to the world in the same manner we always announce releases. It gets sent to the c-ares mailing list and the oss-security mailing list.
- The security web page on the web site should get the new vulnerability mentioned.

C-ARES-SECURITY (at haxx dot se)

Who is on this list? There are a couple of criteria you must meet, and then we might ask you to join the list or you can ask to join it. It really isn't very formal. We basically only require that you have a long-term presence in the c-ares project and you have shown an understanding for the project and its way of working. You must've been around for a good while and you should have no plans in vanishing in the near future.

We do not make the list of partipants public mostly because it tends to vary somewhat over time and a list somewhere will only risk getting outdated.