About coordinated disclosure of security vulnerabilities

In this article

Vulnerability disclosure is a coordinated effort between security reporters and repository maintainers.

About disclosing vulnerabilities in the industry

Vulnerability disclosure is an area where collaboration between vulnerability reporters, such as security researchers, and project maintainers is very important. Both parties need to work together from the moment a potentially harmful security vulnerability is found, right until a vulnerability is disclosed to the world, ideally with a patch available. Typically, when someone lets a maintainer know privately about a security vulnerability, the maintainer develops a fix, validates it, and notifies the users of the project or package.

The initial report of a vulnerability is made privately, and the full details are only published once the maintainer has acknowledged the issue, and ideally made remediations or a patch available, sometimes with a delay to allow more time for the patches to be installed. For more information, see the "OWASP Cheat Sheet Series about vulnerability disclosure" on the OWASP Cheat Sheet Series website.

Best practices for vulnerability reporters

It's good practice to report vulnerabilities privately to maintainers. When possible, as a vulnerability reporter, we recommend you avoid:

- Disclosing the vulnerability publicly without giving maintainers a chance to remediate.
- Bypassing the maintainers.
- Disclosing the vulnerability before a fixed version of the code is available.
- Expecting to be compensated for reporting an issue, where no public bounty program exists.

It's acceptable for vulnerability reporters to disclose a vulnerability publicly after a period of time, if they have tried to contact the maintainers and not received a response, or contacted them and been asked to wait too long to disclose it.

We recommend vulnerability reporters clearly state the terms of their disclosure policy as part of their reporting process. Even if the vulnerability reporter does not adhere to a strict policy, it's a good idea to set clear expectations for maintainers in terms of timelines on intended vulnerability disclosures. For an example of disclosure policy, see the "Security Lab's disclosure policy" on the GitHub Security Lab website.

Best practices for maintainers

As a maintainer, it's good practice to clearly indicate how and where you want to receive reports for vulnerabilities. If this information is not clearly available, vulnerability reporters don't know how to contact you, and may resort to extracting developer email addresses from git commit histories to try to find an appropriate security contact. This can lead to friction, lost reports, or the publication of unresolved reports.

Maintainers should disclose vulnerabilities in a timely manner. If there is a security vulnerability in your repository, we recommend you:

- Treat the vulnerability as a security issue rather than a simple bug, both in your response and your disclosure. For example, you'll need to explicitly mention that the issue is a security vulnerability in the release notes.
- Acknowledge receipt of the vulnerability report as quickly as possible, even if no immediate resources are available for investigation. This sends the message that you are quick to respond and act, and it sets a positive tone for the rest of the interaction between you and the vulnerability reporter.
- Involve the vulnerability reporter when you verify the impact and veracity of the report. It's likely the vulnerability reporter has already spent time considering the vulnerability in a variety of scenarios, some of which you may have not considered yourself.
- Remediate the issue in a way that you see fit, taking any concerns and advice provided by the vulnerability reporter into careful consideration. Often the vulnerability reporter will have knowledge of certain corner cases and remediation bypasses that are easy to miss without a security research background.
- Always acknowledge the vulnerability reporter when you credit the discovery.
- Aim to publish a fix as soon as you can.
- Ensure that you make the wider ecosystem aware of the issue and its remediation when you disclose the vulnerability. It is not uncommon to see cases where a recognized security issue is fixed in the current development branch of a project, but the commit or subsequent release is not explicitly marked as a security fix or release. This can cause problems with downstream consumers.

Publishing the details of a security vulnerability doesn't make maintainers look bad. Security vulnerabilities are present everywhere in software, and users will trust maintainers who have a clear and established process for disclosing security vulnerabilities in their code.

About reporting and disclosing vulnerabilities in projects on GitHub

There are two processes available on GitHub:

- The standard process: Vulnerability reporters get in touch with the repository maintainers, using contact information located in the security policy for the repository. The repository maintainers then create a draft repository advisory if required.
- Private vulnerability reporting: Vulnerability reporters disclose vulnerability details directly and privately to the repository maintainers by proposing a draft repository advisory and providing details of their findings.

Standard process

The process for reporting and disclosing vulnerabilities for projects on GitHub.com is as follows:

If you are a vulnerability reporter (for example, a security researcher) who would like report a vulnerability, first check if there is a security policy for the related repository. For more information, see "Adding a security policy to your repository." If there is one, follow it to understand the process before contacting the security team for that repository.

If there isn't a security policy in place, the most efficient way to establish a private means of communication with maintainers is to create an issue asking for a preferred security contact. It's worth noting that the issue will be immediately publicly visible, so it should not include any information about the bug. Once communication is established, you can suggest the maintainers define a security policy for future use.

> **Note**: *For npm only* - If we receive a report of malware in an npm package, we try to contact you privately. If you don't address the issue in a timely manner, we will disclose it. For more information, see "Reporting malware in an npm package" on the npm Docs website.

If you've found a security vulnerability in GitHub.com, please report the vulnerability through our coordinated disclosure process. For more information, see the GitHub Security Bug Bounty website.

If you are a maintainer, you can take ownership of the process at the very beginning of the pipeline by setting up a security policy for your repository, or otherwise making security reporting instructions clearly available, for example in your project's README file. For information about adding a security policy, see "Adding a security policy to your repository." If there is no security policy, it's likely that a vulnerability reporter will try to email you or otherwise privately contact you. Alternatively, someone may open a (public) issue with details of a security issue.

As a maintainer, to disclose a vulnerability in your code, you first create a draft security advisory in the package's repository in GitHub. Repository security advisories allow repository maintainers to privately discuss and fix a security vulnerability in a project. After collaborating on a fix, repository maintainers can publish the security advisory to publicly disclose the security vulnerability to the project's community. By publishing security advisories, repository maintainers make it easier for their community to update package dependencies and research the impact of the security vulnerabilities. For more information, see "About repository security advisories."

To get started, see "Creating a repository security advisory."

Private vulnerability reporting

Owners and administrators of public repositories can enable private vulnerability reporting on their repositories. For more information, see "Configuring private vulnerability reporting for a repository."

Private vulnerability reporting provides an easy way for vulnerability reporters to privately disclose security risks to repository maintainers, within GitHub, and in a way that immediately notifies the repository maintainers of the issue. For more information for security researchers and repository maintainers, see "Privately reporting a security vulnerability" and "Managing privately reported security vulnerabilities", respectively.

> **Note**: If the repository containing the vulnerability doesn't have private vulnerability reporting enabled, both security researchers and repository maintainers need to follow the instructions described in the "Standard process" section above.

Legal

© 2023 GitHub, Inc. Terms Privacy Status Pricing Expert services Blog