Vulnerability Management

Reporting Vulnerabilities

As mentioned in the [security policy](https://github.com/vllm-project/vllm/tree/main/SECURITY.md), security vulnerabilities may be reported privately to the project via [GitHub](https://github.com/vllm-project/vllm/security/advisories/new).

Vulnerability Management Team

Once a vulnerability has been reported to the project, the Vulnerability Management Team (VMT) is responsible for managing the vulnerability. The VMT is responsible for: \- Triaging the vulnerability. \- Coordinating with reporters and project maintainers on vulnerability analysis and resolution. \- Drafting of security advisories for confirmed vulnerabilities, as appropriate. \- Coordination with project maintainers on a coordinated release of the fix and security advisory.

Security Advisories

Advisories are published via GitHub through the same system used to report vulnerabilities. More information on the process can be found in the [GitHub documentation](https://docs.github.com/en/code-security/security-advisories/working-with-repository-security-advisories/about-repository-security-advisories).

Team Members

We prefer to keep all vulnerability-related communication on the security report on GitHub. However, if you need to contact the VMT directly for an urgent issue, you may contact the following individuals: \- Simon Mo - simon.mo@hey.com \- Russell Bryant - rbryant@redhat.com

Slack Discussion

You may use the `#security` channel in the [VLLM Slack](https://slack.vllm.ai) to discuss security-related topics. However, please do not disclose any vulnerabilities in this channel. If you need to report a vulnerability, please use the GitHub security advisory system or contact a VMT member privately.

Vulnerability Disclosure

The process for disclosing vulnerabilities is the following: \- The VMT will work with the project maintainers to develop a fix for the vulnerability. \- The VMT will coordinate with the reporter and project maintainers to prepare a security

advisory that adequately describes the vulnerability and its impact. \- The VMT will coordinate with the project maintainers to publish a fix and release an update that includes that fix. \- The VMT will publish the security advisory on GitHub. Release notes will be updated to include a reference to the security advisory. The VMT and project maintainers will work to minimize the amount of time in between disclosing any public information about the vulnerability and making a release and advisory available.