Security Policy

Supported versions

The following table describes the versions of this project that are currently supported with security updates:

Version	Supported
4.x	:white_check_mark:
3.x	:x:
2.x	:x:
1.x	:x:

Responsible disclosure security policy

A responsible disclosure policy helps protect users of the project from publicly disclosed security vulnerabilities without a fix by employing a process where vulnerabilities are first triaged in a private manner, and only publicly disclosed after a reasonable time period that allows patching the vulnerability and provides an upgrade path for users.

When contacting us directly via email, we will do our best efforts to respond in a reasonable time to resolve the issue. When contacting a security program their disclosure policy will provide details on time-frame, processes and paid bounties.

We kindly ask you to refrain from malicious acts that put our users, the project, or any of the project’s team members at risk.

Reporting a security issue

We consider the security of our systems a top priority. But no matter how much effort we put into system security, there can still be vulnerabilities present.

If you discover a security vulnerability, please use one of the following means of communications to report it to us:

- Report the security issue to the Node.js Security Working Group through the HackerOne program for ecosystem modules on npm, or to Snyk Security Team. They will help triage the security issue and work with all involved parties to remediate and release a fix.

Note that time-frame and processes are subject to each program’s own policy.

- Report the security issue to the project maintainers directly at security@lodash.com.

Your efforts to responsibly disclose your findings are sincerely appreciated and will be taken into account to acknowledge your contributions.