Security Policy

Supported Versions

Redis is generally backwards compatible with very few exceptions, so we recommend users to always use the latest version to experience stability, performance and security.

We generally backport security issues to a single previous major version, unless this is not possible or feasible with a reasonable effort.

Version	Supported
6.2.x	:white_check_mark:
6.0.x	:white_check_mark:
5.0.x	:white_check_mark:
< 5.0	:x:

Reporting a Vulnerability

If you believe you've discovered a serious vulnerability, please contact the Redis core team at redis@redis.io. We will evaluate your report and if necessary issue a fix and an advisory. If the issue was previously undisclosed, we'll also mention your name in the credits.

Responsible Disclosure

In some cases, we may apply a responsible disclosure process to reported or otherwise discovered vulnerabilities. We will usually do that for a critical vulnerability, and only if we have a good reason to believe information about it is not yet public.

This process involves providing an early notification about the vulnerability, its impact and mitigations to a short list of vendors under a time-limited embargo on public disclosure.

Vendors on the list are individuals or organizations that maintain Redis distributions or provide Redis as a service, who have third party users who will benefit from the vendor's ability to prepare for a new version or deploy a fix early.

If you believe you should be on the list, please contact us and we will consider your request based on the above criteria.