Security

Reporting a bug in Node.js

Report security bugs in Node.js via HackerOne.

Your report will be acknowledged within 5 days, and you'll receive a more detailed response to your report within 10 days indicating the next steps in handling your submission.

After the initial reply to your report, the security team will endeavor to keep you informed of the progress being made towards a fix and full announcement, and may ask for additional information or guidance surrounding the reported issue.

Node.js bug bounty program

The Node.js project engages in an official bug bounty program for security researchers and responsible public disclosures. The program is managed through the HackerOne platform. See https://hackerone.com/nodejs for further details.

Reporting a bug in a third party module

Security bugs in third party modules should be reported to their respective maintainers.

Disclosure policy

Here is the security disclosure policy for Node.js

- The security report is received and is assigned a primary handler. This person will coordinate the fix and release process. The problem is confirmed and a list of all affected versions is determined. Code is audited to find any potential similar problems. Fixes are prepared for all releases which are still under maintenance. These fixes are not committed to the public repository but rather held locally pending the announcement.
- A suggested embargo date for this vulnerability is chosen and a CVE (Common Vulnerabilities and Exposures (CVE®)) is requested for the vulnerability.
- On the embargo date, the Node.js security mailing list is sent a copy of the announcement. The changes are pushed to the public repository and new builds are deployed to nodejs.org. Within 6 hours of the mailing list being notified, a copy of the advisory will be published on the Node.js blog.
- Typically the embargo date will be set 72 hours from the time the CVE is issued. However, this may vary depending on the severity of the bug or difficulty in applying a fix.

- This process can take some time, especially when coordination is required with maintainers of other projects. Every effort will be made to handle the bug in as timely a manner as possible; however, it's important that we follow the release process above to ensure that the disclosure is handled in a consistent manner.

Receiving security updates

Security notifications will be distributed via the following methods.

- https://groups.google.com/group/nodejs-sec
- https://nodejs.org/en/blog/

Comments on this policy

If you have suggestions on how this process could be improved please submit a pull request or file an issue to discuss.