Security release process

The security release process covers the steps required to plan/implement a security release. This document is copied into the description of the Next Security Release and used to track progress on the release. It contains ***TEXT LIKE THIS*** which will be replaced during the release process with the information described.

Security release stewards

For each security release, a security steward will take ownership for coordinating the steps outlined in this process. Security stewards are nominated through an issue in the TSC repository and approved through the regular TSC consensus process. Once approved, they are given access to all of the resources needed to carry out the steps listed in the process as outlined in security steward on/off boarding.

The current security stewards are documented in the main Node.js README.md.

Company	Person	Release Date
NearForm	Matteo	2021-Oct-12
Datadog	Bryan	2022-Jan-10
RH and IBM	Joe	
NearForm	Matteo	
Datadog	Vladimir	
RH and IBM	Michael	

Planning

- □ Open an issue titled `Next Security Release`, and put this checklist in the description.
- □ Get agreement on the list of vulnerabilities to be addressed:
  - ***H1 REPORT LINK***: ***DESCRIPTION*** (***CVE or H1 CVE request link***)
    - v10.x, v12.x: ***LINK to PR URL***
  - …
- □ PR release announcements in private:
  - (Use previous PRs as templates. Don't forget to update the site banner and the date in the slug so that it will move to the top of the blog list.)
  - □ pre-release: ***LINK TO PR***
  - □ post-release: ***LINK TO PR***
    - List vulnerabilities in order of descending severity
    - Ask the HackerOne reporter if they would like to be credited on the security release blog page:

```
Thank you to <name> for reporting this vulnerability.
```

- □ Get agreement on the planned date for the release: ***RELEASE DATE***
- □ Get release team volunteers for all affected lines:
  - v12.x: ***NAME of RELEASER(S)***
  - … other lines, if multiple releasers

Announcement (one week in advance of the planned release)

- □ Verify that GitHub Actions are working as normal: https://www.githubstatus.com/.
- □ Check that all vulnerabilities are ready for release integration:
  - PRs against all affected release lines or cherry-pick clean
  - Approved
  - Pass `make test`
  - Have CVEs
    - Make sure that dependent libraries have CVEs for their issues. We should only create CVEs for vulnerabilities in Node.js itself. This is to avoid having duplicate CVEs for the same vulnerability.
  - Described in the pre/post announcements
- □ Pre-release announcement to nodejs.org blog: ***LINK TO BLOG*** (Re-PR the pre-approved branch from nodejs-private/nodejs.org-private to nodejs/nodejs.org)

  If the security release will only contain an OpenSSL update consider adding the following to the pre-release announcement:

  ```
  Since this security release will only include updates for OpenSSL, if you're using
  a Node.js version which is part of a distribution which uses a system
  installed OpenSSL, this Node.js security update might not concern you. You may
  instead need to update your system OpenSSL libraries, please check the
  security announcements for the distribution.
  ```
- □ Pre-release announcement email: ***LINK TO EMAIL***
  - Subject: `Node.js security updates for all active release lines, Month Year`
  - Body:

  ```
  The Node.js project will release new versions of all supported release lines on or shor
  For more information see: https://nodejs.org/en/blog/vulnerability/month-year-security-
  ```

  (Get access from existing manager: Matteo Collina, Rodd Vagg, Michael Dawson, Bryan English, Vladimir de Turckheim)
- □ CC `oss-security@lists.openwall.com` on pre-release

The google groups UI does not support adding a CC, until we figure out a better way, forward the email you receive to `oss-security@lists.openwall.com` as a CC.

- □ Create a new issue in nodejs/tweet

  ```
  Security release pre-alert:

  We will release new versions of <add versions> release lines on or shortly
  after Day Month Date, Year in order to address:

  - # high severity issues
  - # moderate severity issues

  https://nodejs.org/en/blog/vulnerability/month-year-security-releases/
  ```

- □ Request releaser(s) to start integrating the PRs to be released.
- □ Notify docker-node of upcoming security release date: ***LINK***

  ```
  Heads up of Node.js security releases Day Month Year

  As per the Node.js security release process this is the FYI that there is going to be a
  ```

- □ Notify build-wg of upcoming security release date by opening an issue in nodejs/build to request WG members are available to fix any CI issues.

  ```
  Heads up of Node.js security releases Day Month Year

  As per security release process this is a heads up that there will be security releases
  ```

Release day

- □ Lock CI
- □ The releaser(s) run the release process to completion.
- □ Unlock CI
- □ Post-release announcement to Nodejs.org blog: ***LINK TO BLOG POST***
  - (Re-PR the pre-approved branch from nodejs-private/nodejs.org-private to nodejs/nodejs.org)
- □ Post-release announcement in reply email: ***LINK TO EMAIL***
  - CC: `oss-security@lists.openwall.com`
  - Subject: `Node.js security updates for all active release lines, Month Year`
  - Body:

  ```
  The Node.js project has now released new versions of all supported release lines.
  For more information see: https://nodejs.org/en/blog/vulnerability/month-year-security-
  ```

□ Create a new issue in nodejs/tweet

```
Security release:

New security releases are now available for versions <add versions> of Node.js.

https://nodejs.org/en/blog/vulnerability/month-year-security-releases/
```

□ Comment in docker-node issue that release is ready for integration. The docker-node team will build and release docker image updates.

□ For every H1 report resolved:

- Close as Resolved
- Request Disclosure
- Request publication of H1 CVE requests
  - (Check that the "Version Fixed" field in the CVE is correct, and provide links to the release blogs in the "Public Reference" section)

□ PR machine-readable JSON descriptions of the vulnerabilities to the core vulnerability DB. ***LINK TO PR***

- For each vulnerability add a `#.json` file, one can copy an existing json file, and increment the latest created file number and use that as the name of the new file to be added. For example, `79.json`.

□ Close this issue

□ Make sure the PRs for the vulnerabilities are closed.