Security WG meeting 2017-11-02

GitHub issue: https://github.com/nodejs/security-wg/issues/63
Meeting video: https://youtu.be/UWKC1GTPAFo
Previous meeting:
https://github.com/nodejs/security-wg/blob/master/meetings/2017-10-12.md

Present
- Bryan English (@bengl)
- Sam Roberts (@sam-github)
- Vladimir de Turckheim (@vdeturckheim)
- Michael Alexander (@mgalexander)
- Michael Dawson (@mhdawson)
- Reed Loden (@reedloden)
- Colin Ihrig (@cjihrig)
- Arunesh Chandra (@aruneshchandra)-observer
- Hitesh Kanwathirtha (@digitalinfinity)-observer
- Adam Baldwin - late (@evilpacket)

Review of last meeting

New agenda

HackerOne setup/demo

* @vdeturckheim gave us a walkthrough of what he has setup.
* Easy to invite people to collaborate on specific vulnerabilities
*

Bug Bounty Program https://github.com/nodejs/security-wg/issues/49

* want to add bounties Node.js to list they provide bounties for.
* not a huge amount of money ($1500 at the top end)
* does provide some additional motivation for researchers to find/report Issues.
* There is no cost to the project (Internet bug bounty would provide for free)
* Only for security vulnerabilities, do they need to go through HackerOne.
* Needs to meet some minimum bar.
* Michael: should probably get HackerOne setup done first ?
* Michael Alexander volunteered to champion this on the Security-wg, like with an

end of year timeframe.

Proposing an Early Disclosure Program https://github.com/nodejs/security-wg/issues/58

* One thing discussed was to get more input from the potential consumers
* Vladimir will put together and issue, twitter etc to try to gather that input.

acknowledge privacy of info in private repos.https://github.com/nodejs/security-wg/issues/64

* general consensus that having document and having people acknowledge in issue 64 is good enough

Actions
* @vdeturckheim to set up meeting with Core triage team to handover HackerOne Organization (https://github.com/nodejs/security-wg/blob/master/processes/security_team_members.md#team-that-triages-security-reports-against-node-core)
    * Discuss issue linked with potential confusion between 2 HackerOne orgs from security reporters
* @vdeturckheim to create email alias for 3rd party vulnerability report
* @vdeturckheim to open an issue to open an issue to collect inputs regarding early disclosure.
* @mgalexander prepare proposal for bug bounty
* @bengl agreed ~~to socialize the discussion around security team membership (need to confirm)~~ to PR security team membership policy

Document history

14:00 CDT - document opened for group edit
15:30 CDT - initial PR with content as it sits -- minor updates based on @bengl comment
19:00 CDT - locked access to comment
Closing