chrome

When ~~logs~~log list users go bad

breakage from a transparency library misconfiguration, and what we're doing about it

Joe DeBlasio
jdeblasio@chromium.org

Oct 2025

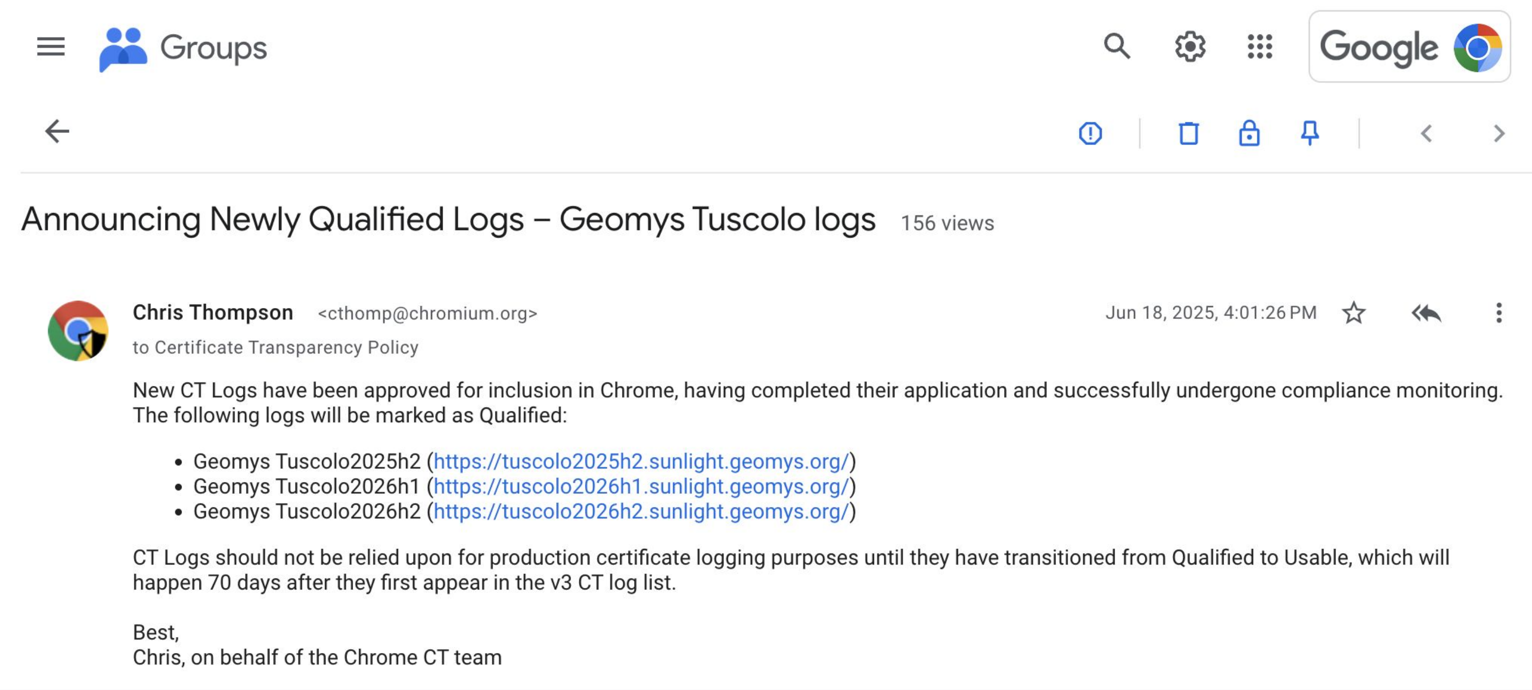
Transparency.dev
Summit 2025

And you are...?

Engineering Manager on **Chrome's Network Security team**

Think CT, HSTS, HTTPS-by-default, revocation, other WebPKI.

oh look it's me



Announcing Newly Qualified Logs – Geomys Tuscolo logs 156 views

Chris Thompson <cthomp@chromium.org> Jun 18, 2025, 4:01:26 PM

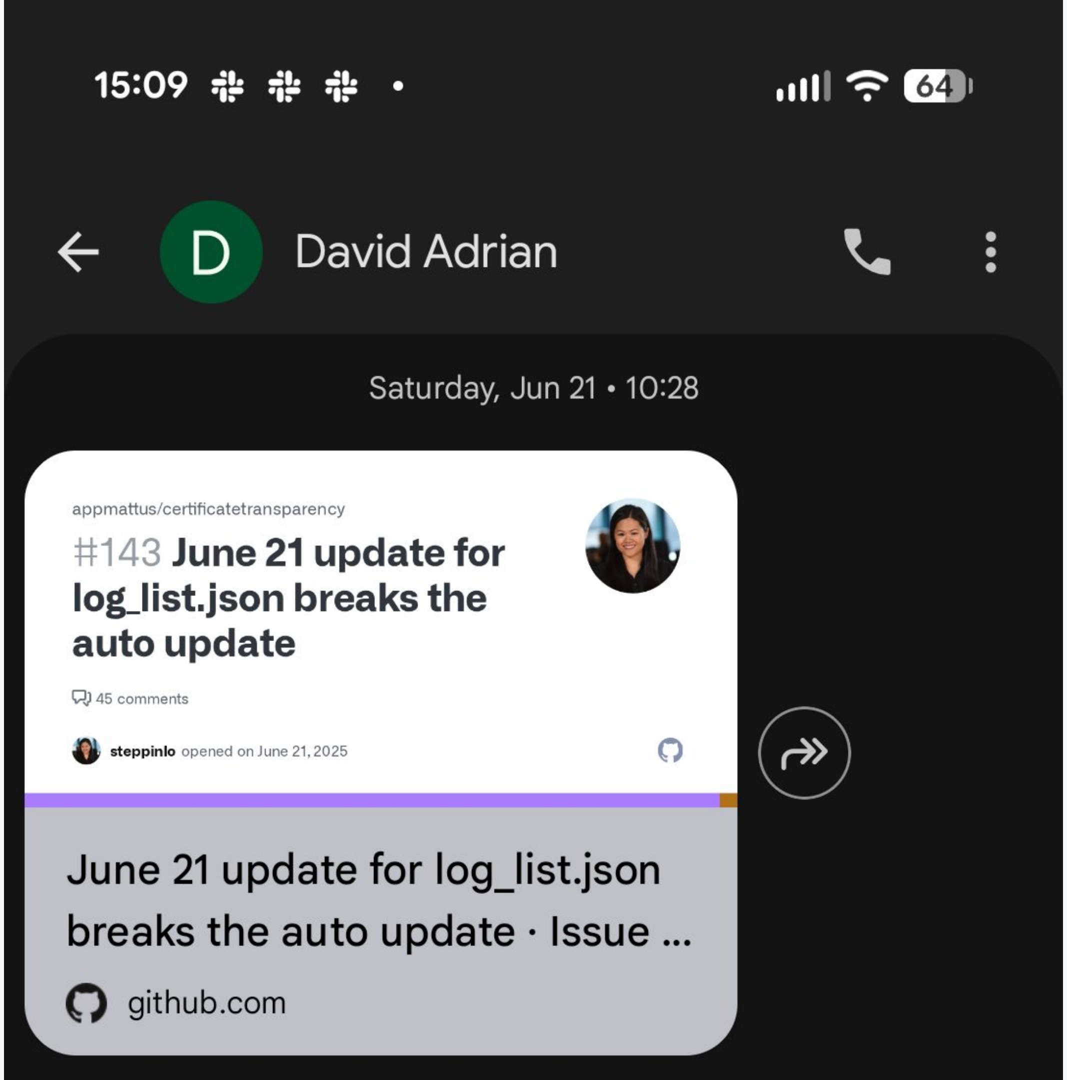
to Certificate Transparency Policy

New CT Logs have been approved for inclusion in Chrome, having completed their application and successfully undergone compliance monitoring. The following logs will be marked as Qualified:

- Geomys Tuscolo2025h2 (https://tuscolo2025h2.sunlight.geomys.org/)
- Geomys Tuscolo2026h1 (https://tuscolo2026h1.sunlight.geomys.org/)
- Geomys Tuscolo2026h2 (https://tuscolo2026h2.sunlight.geomys.org/)

CT Logs should not be relied upon for production certificate logging purposes until they have transitioned from Qualified to Usable, which will happen 70 days after they first appear in the v3 CT log list.

Best,
Chris, on behalf of the Chrome CT team



Saturday, Jun 21 • 10:28

appmattus/certificatetransparency

#143 **June 21 update for log_list.json breaks the auto update**

45 comments

steppinlo opened on June 21, 2025

June 21 update for log_list.json breaks the auto update · Issue ...

github.com

A bunch of Android apps broke…

Impacted tens of millions of users…

- McDonald's
- Lowe's
- Deutsche Telekom
- UPS
- A bunch of banks
- Many more…

As soon as you opened an impacted app, the app would crash.

Chrome's Log List

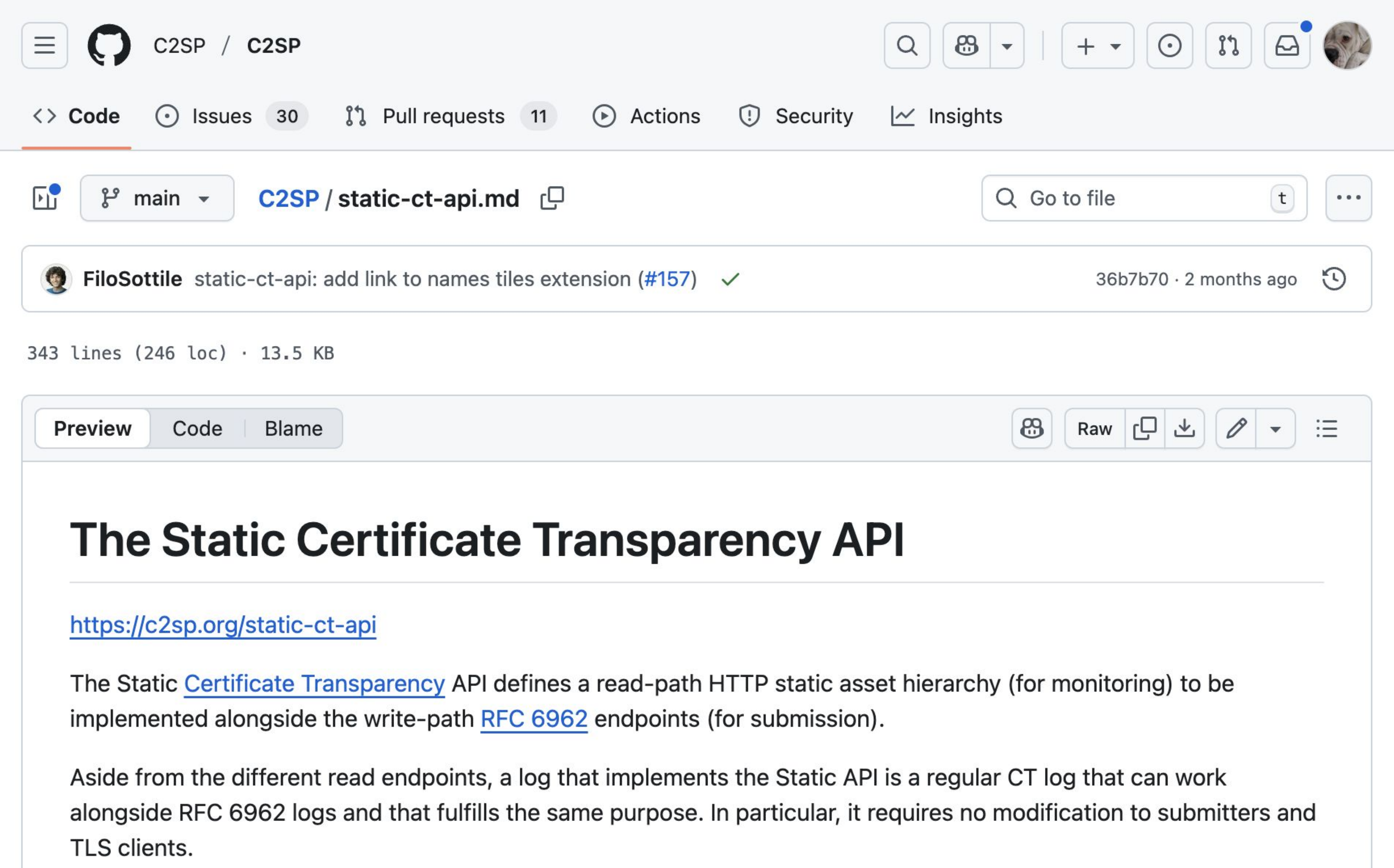
We publish a json list of logs that Chrome recognizes so that people can...

- assemble cert+SCTs that validate in Chrome,
- know what logs can be used to detect missisuance used against Chrome users,
- help keep logs honest.

It's ***not*** so that CT enforcing UAs can just "do what Chrome does".

- Other well behaved user agents (e.g. Apple) publish their own log lists.
- Other UAs *can* derive their lists from ours (Android, Firefox, etc), but care needs to be taken.

Otherwise, you take on risk for your UA *and* risk for the ecosystem.



FiloSottile static-ct-api: add link to names tiles extension (#157) ✓ 36b7b70 · 2 months ago

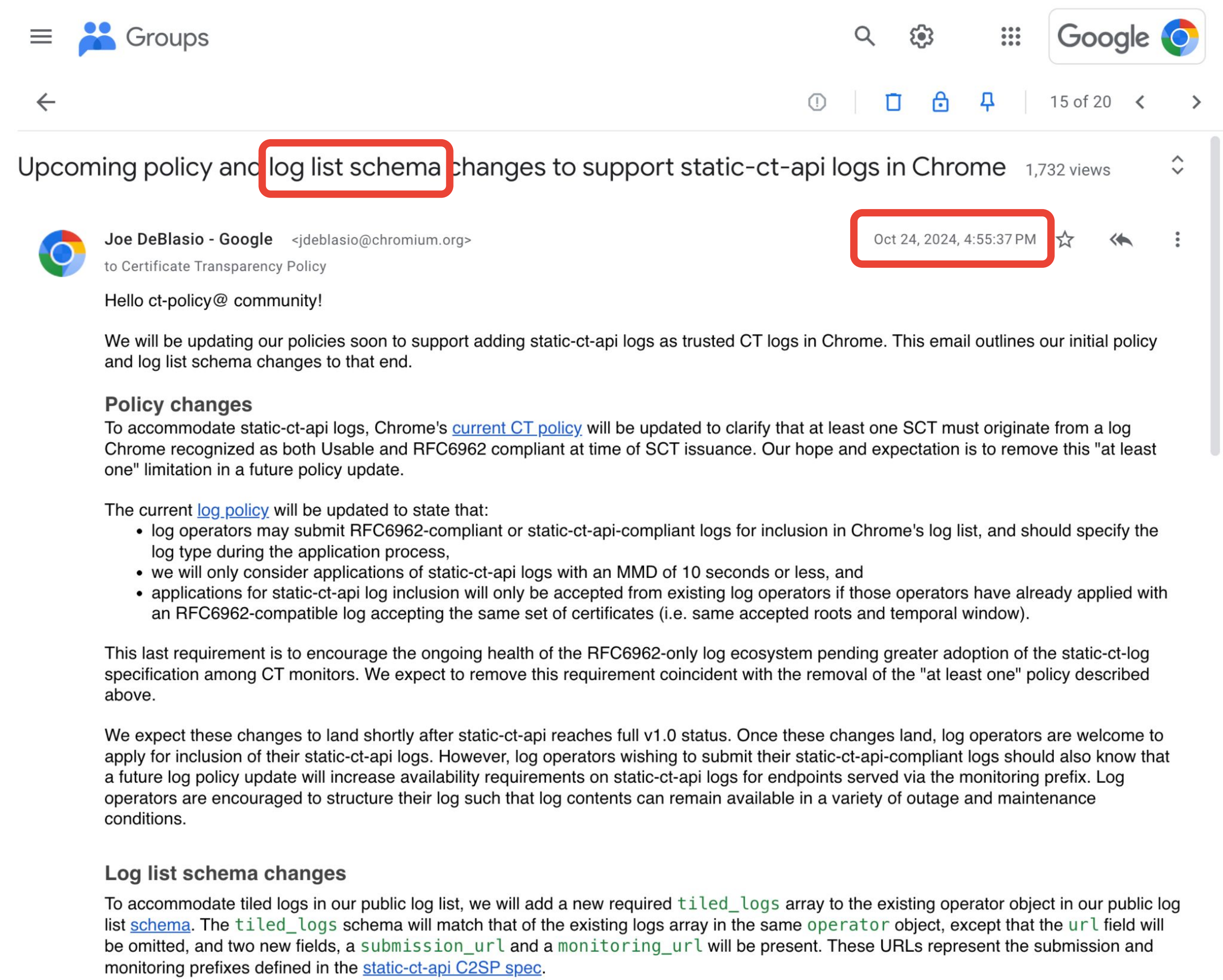
343 lines (246 loc) · 13.5 KB

The Static Certificate Transparency API

https://c2sp.org/static-ct-api

The Static Certificate Transparency API defines a read-path HTTP static asset hierarchy (for monitoring) to be implemented alongside the write-path RFC 6962 endpoints (for submission).

Aside from the different read endpoints, a log that implements the Static API is a regular CT log that can work alongside RFC 6962 logs and that fulfills the same purpose. In particular, it requires no modification to submitters and TLS clients.



Upcoming policy and log list schema changes to support static-ct-api logs in Chrome

1,732 views

Joe DeBlasio - Google <jdeblasio@chromium.org>
to Certificate Transparency Policy

Oct 24, 2024, 4:55:37 PM

Hello ct-policy@ community!

We will be updating our policies soon to support adding static-ct-api logs as trusted CT logs in Chrome. This email outlines our initial policy and log list schema changes to that end.

Policy changes

To accommodate static-ct-api logs, Chrome's current CT policy will be updated to clarify that at least one SCT must originate from a log Chrome recognized as both Usable and RFC6962 compliant at time of SCT issuance. Our hope and expectation is to remove this "at least one" limitation in a future policy update.

The current log policy will be updated to state that:

- log operators may submit RFC6962-compliant or static-ct-api-compliant logs for inclusion in Chrome's log list, and should specify the log type during the application process,
- we will only consider applications of static-ct-api logs with an MMD of 10 seconds or less, and
- applications for static-ct-api log inclusion will only be accepted from existing log operators if those operators have already applied with an RFC6962-compatible log accepting the same set of certificates (i.e. same accepted roots and temporal window).

This last requirement is to encourage the ongoing health of the RFC6962-only log ecosystem pending greater adoption of the static-ct-log specification among CT monitors. We expect to remove this requirement coincident with the removal of the "at least one" policy described above.

We expect these changes to land shortly after static-ct-api reaches full v1.0 status. Once these changes land, log operators are welcome to apply for inclusion of their static-ct-api logs. However, log operators wishing to submit their static-ct-api-compliant logs should also know that a future log policy update will increase availability requirements on static-ct-api logs for endpoints served via the monitoring prefix. Log operators are encouraged to structure their log such that log contents can remain available in a variety of outage and maintenance conditions.

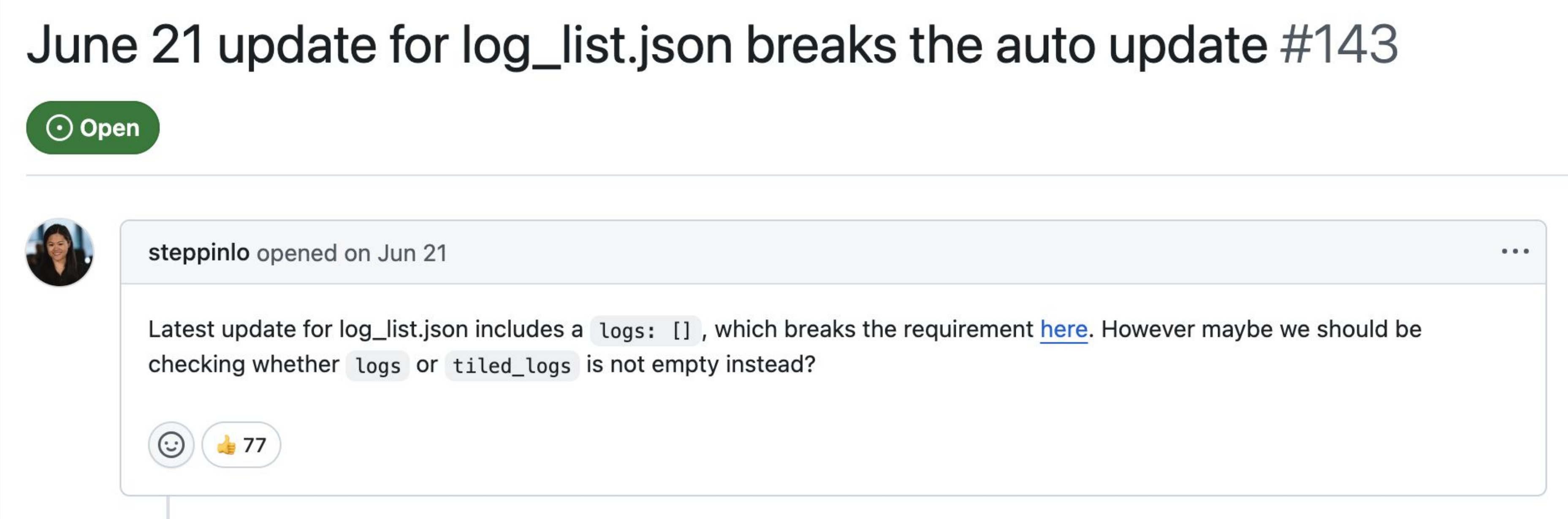
Log list schema changes

To accommodate tiled logs in our public log list, we will add a new required `tiled_logs` array to the existing operator object in our public log list schema. The `tiled_logs` schema will match that of the existing logs array in the same `operator` object, except that the `url` field will be omitted, and two new fields, a `submission_url` and a `monitoring_url` will be present. These URLs represent the submission and monitoring prefixes defined in the static-ct-api C2SP spec.

appmattus/certificatetransparency

Open source library, available on GitHub, for enforcing CT for Android and Java

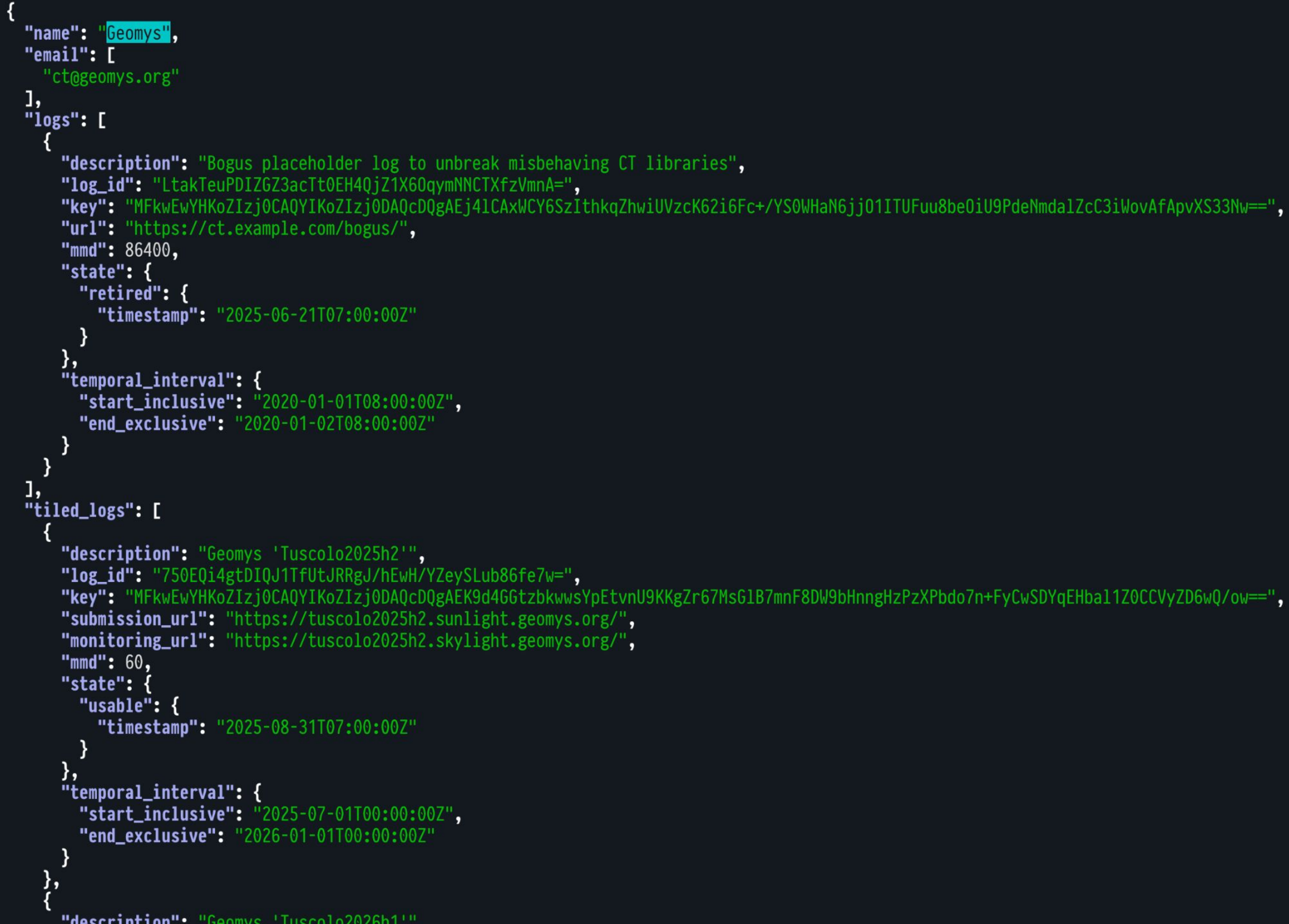
- Fills a niche! Android didn't have native support for CT until Android 16!
- Now developed and maintained by one individual, in his spare time.
- Piggybacks on Chrome's log list -- every client fetches the list at app start.
- Has very strict schema and signature enforcement -- crashes when format doesn't match what's expected.



June 21 update for log_list.json breaks the auto update #143

steppinlo opened on Jun 21

Latest update for log_list.json includes a `logs: []`, which breaks the requirement here. However maybe we should be checking whether `logs` or `tiled_logs` is not empty instead?



```
{
  "name": "Geomys",
  "email": [
    "ct@geomys.org"
  ],
  "logs": [
    {
      "description": "Bogus placeholder log to unbreak misbehaving CT libraries",
      "log_id": "LtakTeuPDIZGZ3acTt0EH4QjZ1X6OqymNNCTXfzVmnA=",
      "key": "MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEj4lCAxWCY6SzIthkqZhwiUVzcK62i6Fc+/YS0WHaN6jjO1ITUFuu8beOiU9PdeNmdalZcC3iWovAfApvXS33Nw==",
      "url": "https://ct.example.com/bogus/",
      "mmd": 86400,
      "state": {
        "retired": {
          "timestamp": "2025-06-21T07:00:00Z"
        }
      },
      "temporal_interval": {
        "start_inclusive": "2020-01-01T08:00:00Z",
        "end_exclusive": "2020-01-02T08:00:00Z"
      }
    }
  ],
  "tiled_logs": [
    {
      "description": "Geomys 'Tuscolo2025h2'",
      "log_id": "75OEQi4gtDIQJ1TfUtJRRgJ/hEwH/YZeySLub86fe7w=",
      "key": "MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEK9d4GGtzbkwwsYpEtvnU9KKgZr67MsGlB7mnF8DW9bHnngHzPzXPbdo7n+FyCwSDYqEHbal1Z0CCVyZD6wQ/ow==",
      "submission_url": "https://tuscolo2025h2.sunlight.geomys.org/",
      "monitoring_url": "https://tuscolo2025h2.skylight.geomys.org/",
      "mmd": 60,
      "state": {
        "usable": {
          "timestamp": "2025-08-31T07:00:00Z"
        }
      },
      "temporal_interval": {
        "start_inclusive": "2025-07-01T00:00:00Z",
        "end_exclusive": "2026-01-01T00:00:00Z"
      }
    },
    {
      "description": "Geomys 'Tuscolo2026h1'",
```

Déjà vu

In 2022, we changed our log list schema, and the *same library* crashed

Roger Ng, here today, gave a lightning talk at CATS 2023 on this failure last time!

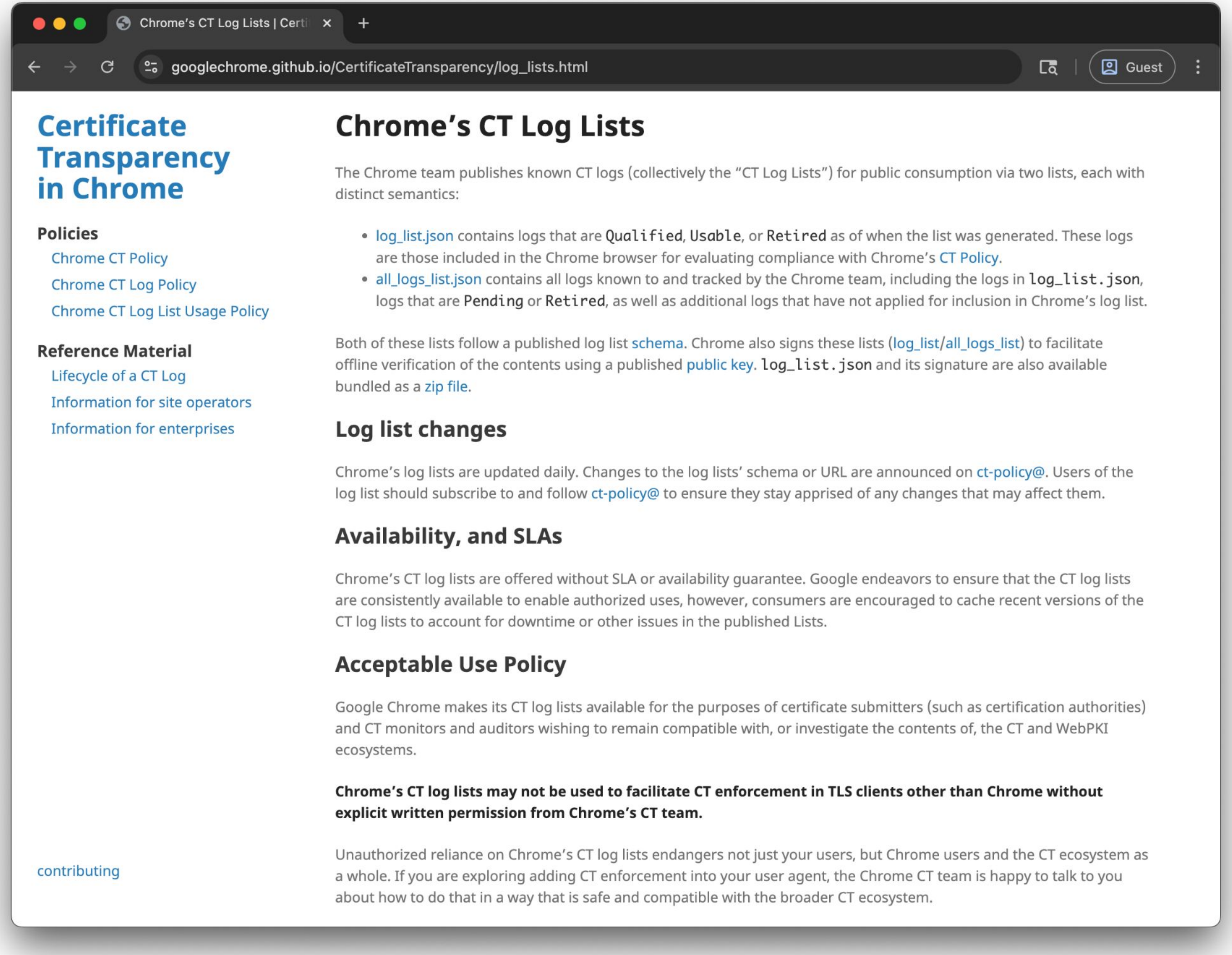
Certificate Transparency Log Lists

Lightning Talk for CATS 2023

Google Certificate Transparency Team

Roger Ng
rogerng@google.com

Nov 2023


Chrome's CT Log Lists | Certi
googlechrome.github.io/CertificateTransparency/log_lists.html
Guest

Certificate Transparency in Chrome

Policies

- Chrome CT Policy
- Chrome CT Log Policy
- Chrome CT Log List Usage Policy

Reference Material

- Lifecycle of a CT Log
- Information for site operators
- Information for enterprises

contributing

Chrome's CT Log Lists

The Chrome team publishes known CT logs (collectively the "CT Log Lists") for public consumption via two lists, each with distinct semantics:

- log_list.json contains logs that are `Qualified`, `Usable`, or `Retired` as of when the list was generated. These logs are those included in the Chrome browser for evaluating compliance with Chrome's CT Policy.
- all_logs_list.json contains all logs known to and tracked by the Chrome team, including the logs in `log_list.json`, logs that are `Pending` or `Retired`, as well as additional logs that have not applied for inclusion in Chrome's log list.

Both of these lists follow a published log list schema. Chrome also signs these lists (log_list/all_logs_list) to facilitate offline verification of the contents using a published public key. `log_list.json` and its signature are also available bundled as a zip file.

Log list changes

Chrome's log lists are updated daily. Changes to the log lists' schema or URL are announced on ct-policy@. Users of the log list should subscribe to and follow ct-policy@ to ensure they stay apprised of any changes that may affect them.

Availability, and SLAs

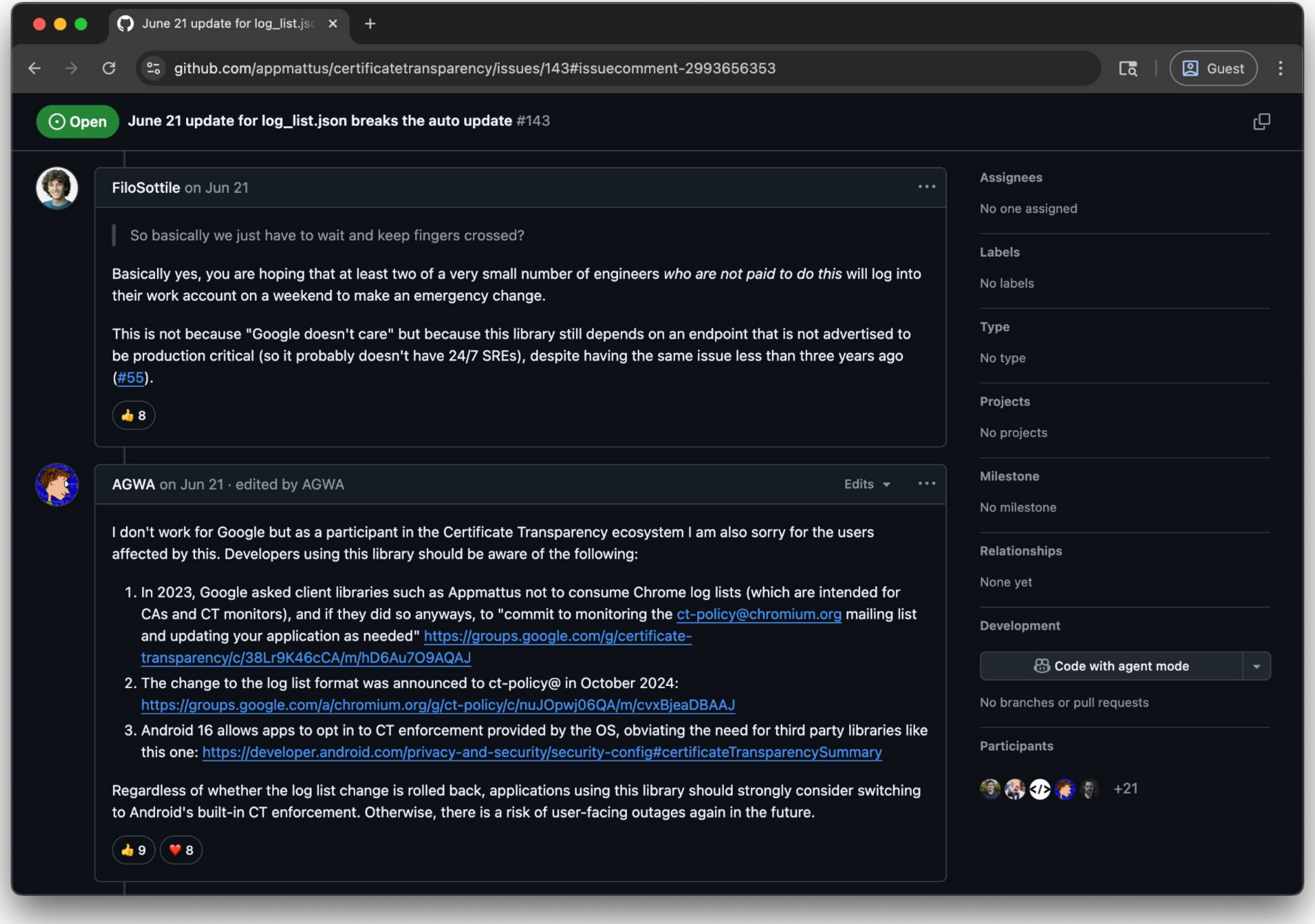
Chrome's CT log lists are offered without SLA or availability guarantee. Google endeavors to ensure that the CT log lists are consistently available to enable authorized uses, however, consumers are encouraged to cache recent versions of the CT log lists to account for downtime or other issues in the published Lists.

Acceptable Use Policy

Google Chrome makes its CT log lists available for the purposes of certificate submitters (such as certification authorities) and CT monitors and auditors wishing to remain compatible with, or investigate the contents of, the CT and WebPKI ecosystems.

Chrome's CT log lists may not be used to facilitate CT enforcement in TLS clients other than Chrome without explicit written permission from Chrome's CT team.

Unauthorized reliance on Chrome's CT log lists endangers not just your users, but Chrome users and the CT ecosystem as a whole. If you are exploring adding CT enforcement into your user agent, the Chrome CT team is happy to talk to you about how to do that in a way that is safe and compatible with the broader CT ecosystem.


June 21 update for log_list.jsc
github.com/appmattus/certificatetransparency/issues/143#issuecomment-2993656353
Guest

Open **June 21 update for log_list.json breaks the auto update** #143

FiloSottile on Jun 21

> So basically we just have to wait and keep fingers crossed?

Basically yes, you are hoping that at least two of a very small number of engineers *who are not paid to do this* will log into their work account on a weekend to make an emergency change.

This is not because "Google doesn't care" but because this library still depends on an endpoint that is not advertised to be production critical (so it probably doesn't have 24/7 SREs), despite having the same issue less than three years ago (#55).

👍 8

AGWA on Jun 21 · edited by AGWA

Edits ▾

I don't work for Google but as a participant in the Certificate Transparency ecosystem I am also sorry for the users affected by this. Developers using this library should be aware of the following:

1. In 2023, Google asked client libraries such as Appmattus not to consume Chrome log lists (which are intended for CAs and CT monitors), and if they did so anyways, to "commit to monitoring the ct-policy@chromium.org mailing list and updating your application as needed" https://groups.google.com/g/certificate-transparency/c/38Lr9K46cCA/m/hD6Au7O9AQAJ
2. The change to the log list format was announced to ct-policy@ in October 2024: https://groups.google.com/a/chromium.org/g/ct-policy/c/nuJOpwj06QA/m/cvxBjeaDBAAJ
3. Android 16 allows apps to opt in to CT enforcement provided by the OS, obviating the need for third party libraries like this one: https://developer.android.com/privacy-and-security/security-config#certificateTransparencySummary

Regardless of whether the log list change is rolled back, applications using this library should strongly consider switching to Android's built-in CT enforcement. Otherwise, there is a risk of user-facing outages again in the future.

👍 9 ❤️ 8

Assignees

No one assigned

Labels

No labels

Type

No type

Projects

No projects

Milestone

No milestone

Relationships

None yet

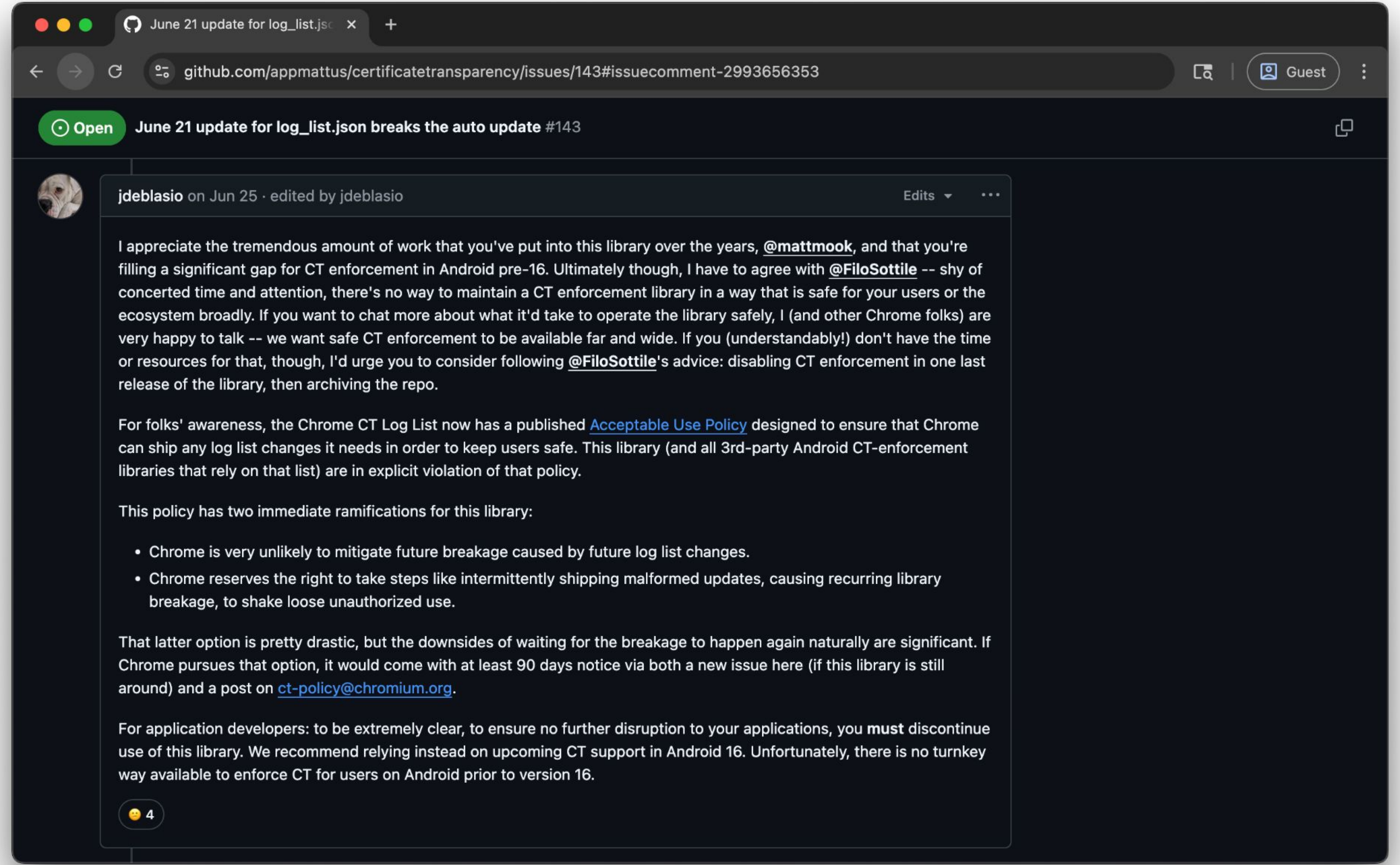
Development

Code with agent mode ▾

No branches or pull requests

Participants

+21


June 21 update for log_list.jsc
github.com/appmattus/certificatetransparency/issues/143#issuecomment-2993656353
Guest

Open June 21 update for log_list.json breaks the auto update #143

jdeblasio on Jun 25 · edited by jdeblasio

I appreciate the tremendous amount of work that you've put into this library over the years, **@mattmook**, and that you're filling a significant gap for CT enforcement in Android pre-16. Ultimately though, I have to agree with **@FiloSottile** -- shy of concerted time and attention, there's no way to maintain a CT enforcement library in a way that is safe for your users or the ecosystem broadly. If you want to chat more about what it'd take to operate the library safely, I (and other Chrome folks) are very happy to talk -- we want safe CT enforcement to be available far and wide. If you (understandably!) don't have the time or resources for that, though, I'd urge you to consider following **@FiloSottile**'s advice: disabling CT enforcement in one last release of the library, then archiving the repo.

For folks' awareness, the Chrome CT Log List now has a published Acceptable Use Policy designed to ensure that Chrome can ship any log list changes it needs in order to keep users safe. This library (and all 3rd-party Android CT-enforcement libraries that rely on that list) are in explicit violation of that policy.

This policy has two immediate ramifications for this library:

- Chrome is very unlikely to mitigate future breakage caused by future log list changes.
- Chrome reserves the right to take steps like intermittently shipping malformed updates, causing recurring library breakage, to shake loose unauthorized use.

That latter option is pretty drastic, but the downsides of waiting for the breakage to happen again naturally are significant. If Chrome pursues that option, it would come with at least 90 days notice via both a new issue here (if this library is still around) and a post on ct-policy@chromium.org.

For application developers: to be extremely clear, to ensure no further disruption to your applications, you **must** discontinue use of this library. We recommend relying instead on upcoming CT support in Android 16. Unfortunately, there is no turnkey way available to enforce CT for users on Android prior to version 16.

😕 4

Getting pushier

Starting next year we will be...

- Working with Play Store to warn, block updates for, offending Android apps, then
- Reaching out to developers of major apps directly, then
- Breaking requests for our log list that come from these apps.

So if you're an Android app developer...

- Don't rely on third-party CT enforcement.
- Enforce CT on Android 16+ by opting-in to platform enforcement.
- Don't enforce CT on prior versions of Android.

So if you develop a TLS client that wants to enforce CT

- Can you commit to running a proper CT log program?
- If not, PLEASE don't blindly rely on other UA's lists! Talk to us! We're friendly.
- Unfortunately, we will try to break unauthorized dependencies.

Questions?

You can also email us!
jdeblasio@chromium.org
chrome-certificate-transparency@google.com