Main page
Recent changes
Server admin log (Prod)
Server admin log (RelEng)
Deployments
SRE/Operations Help
Incident status

Cloud VPS & Toolforge
Cloud VPS documentation
Toolforge documentation
Request Cloud VPS project
Server admin log (Cloud VPS)

Tools
What links here
Related changes
Special pages
Permanent link
Page information
Cite this page

Print/export
Create a book
Download as PDF
Printable version

Incident documentation/20161013-GlobalSign

< Incident documentation

Summary

On Oct 13th, the CA providing our primary TLS certificates, GlobalSign, had a very costly technical/process failure which lead to some User-Agents viewing their intermediate signing certificates as being Revoked, which in turn caused those User-Agents to not to trust the authenticity of Wikimedia's primary site certificates. Many other sites aside from ours were affected as well. We were eventually able to mitigate the issue hours later with a workaround delivered by GlobalSign.

Impacted Users

- Only certain modern UAs were affected (older ones don't check OCSP, especially on Intermediates).
  - Definitely affected greatly: Safari+Chrome on macOS Sierra (new OS release less than 1 month ago)
  - Potentially affected: (user reports varied, or were intermittent): Edge and/or IE on Win10, Safari on iOS 10, OperaMini?
- Note also that the effect on users would ramp in slowly over time as the incident drags on, because they don't constantly check for the problematic OCSP response. This is why, for all involved, the problem looked so much smaller at the start of the timeline than it did towards the end.
- There was no substantial/notable/sharp dropoff in our overall request rates during the incident, which leads us to believe the affected UAs were a small (but vocal) minority.

Other Links

- GlobalSign's Official Incident Report: https://downloads.globalsign.com/acton/attachment/2674/f-06d2/1/-/-/-/-/globalsign-incident-report-13-oct-2016.pdf?utm_term=GlobalSign%2013%20October%202016%20Incident%20Report&utm_campaign=GlobalSign%20Important%20Communication%20-%20Incident%20Report&utm_content=email&utm_source=Act-On+Software&utm_medium=email&sid=TV2:w8wwxT2cx
- General public links on the incident:
  - http://www.theregister.co.uk/2016/10/13/globalsigned_off/
  - http://www.zdnet.com/article/globalsign-security-certificate-foul-up-knocks-out-secure-websites/
  - https://twitter.com/globalsign/status/786505261842247680
  - https://www.globalsign.com/en/customer-revocation-error/
  - https://www.neowin.net/news/https-websites-secured-with-globalsign-certificates-become-inaccessible
- Our public twitter posts on the incident:
  - https://twitter.com/Wikipedia/status/786582520582115328
  - https://twitter.com/Wikipedia/status/786597464555991043
- Task that eventually started tracking related things in realtime:
  - Task T148045

Timeline

All times UTC:

- 10:00 - Claimed actual start time by GlobalSign: https://www.globalsign.com/en/status/
- 11:30 - first reports about anything related on IRC, nobody in ops really notices them yet
- 12:00-14:00 - a trickle of user reports of issues that increasingly point at a real problem for us, lots of technical digging, the answers we find aren't making sense as we seem to be able to confirm our OCSP Staples are working correctly (for the leaf certificates!). During the earlier part of this period we're really not sure if we're significantly affected at all. During the latter part we're pretty sure we are but still can't quite explain how. All communication is via IRC up to this point.
- 14:17 - First email response to Ops list and Toby, overly verbose, describing the current state of investigation with lots of outstanding question-marks.
- 14:20 - First reproductions we can work with to really debug on IRC (our own techops staff reproducing the issue, on MacOS Sierra)
- 14:30 - We start attempting to contact GlobalSign account rep directly for more info (by phone, email)
- 14:35 - Faidon finds data from other investigations on the internet which *finally* point us at the real nature of the problem - that it's an OCSP revocation of the Intermediate signing cert (we had been looking at the leaf this whole time; with nothing better to go on it was a reasonable assumption).
- 14:35-16:10 ... long period of lots of frenzied further investigations and communications, but ultimately we're waiting on GlobalSign, as it's not something we can fix locally ...
- 16:10 - No effective mitigation from GlobalSign, and noticing that the bad revocation could last in user-level caches up to 4 days, we started contacting an alternate vendor about purchasing a replacement cert (this proceeds in parallel from here out as a backup plan).
- 16:52 - GlobalSign informs us of the same 4-day-caching problem, and also say they'll be providing customers with an alternate CA certificate to use to workaround the issue, but haven't actually provided it yet.
- 17:05 - GlobalSign sends us the "Alternate CA" workaround file directly by email from our rep.
- 17:05-17:35 - Examining the file, figuring out how to use it, debating whether we'll break other currently-unaffected clients by using it (or by deploying it improperly), test-deploying it on a canary server and trying that with affected and unaffected browsers, doing the actual deployment of it.
- 17:36 - Workaround intermediate cert fully deployed, seems to immediately fix many (but not all) of the complaining users we have direct contact with. Note the fix is initially deployed only for the critical unified cert (all the production cache clusters and wikis), whereas one-off technical sites (e.g. lists.wikimedia.org, icinga.wikimedia.org, wikitech.wikimedia.org, etc) are not yet fixed initially.
- 17:46 - Additional follow-up deploy step (forced refresh of local OCSP caches) seems to fix remaining complaints, although we don't know if the fix itself was necessary or it was just a timing coincidence and they all would've been fixed regardless by now.
- 19:05 - Smaller one-off technical sites are also all fixed by now
- 19:27 - Hashar reports that our OCG (PDF rendering) service has been broken by the fixed intermediate certs deployed @ 17:36. Investigation indicates this is because it runs a build of node.js with a compiled-in set of Root CAs which lack a critical one from 2009 (in this respect, this version of node.js seems to be worse-off than even ancient real UAs like IE8-on-XP, which have said Root CA).
- 20:00 - Very approximate estimate of the outside (latest) time we could have had a newly-purchased alternate-vendor cert fully deployed (the backup plan, had GlobalSign not delivered a mitigating solution), based on our communications timeline with them and the degree to which work (and progress) on the primary solution slowed that process down on our end.
- 21:26 - OCG sub-issue resolved (by patching and building a new custom node.js package and deploying it to the OCG servers)

Conclusions

- This was an unfortunate blunder on GlobalSign's part, which had limited (to certain newer clients) effects on a broad array of major sites on the Internet.
- It's interesting that lack of direct control by GlobalSign over their CDN provider Cloudflare (which services the affected OCSP traffic for them) seems to have been a significant factor slowing down GlobalSign's ability to deal with this issue.
- While these issues are rare, we can and should be better-equipped to deal with them without being dependent on third parties and blocking on vendor support or purchasing. The ideal solution here is to always purchase and deploy our major certs from two separate vendors in parallel, so that we can disable one or the other in cases like these and fix things quickly. We had considered this in the past, but only as part of our larger undone work towards HPKP. It makes sense to get it done separately from and with more priority than our eventual HPKP work. The cost and complexity of doing so is not unreasonable given the benefits and major risks of not having an alternative.

Actionables

- Mitigate the main issue in the present (Task T148045)
  - Followup fixes for one-off sites: (Task T148069)
  - Followup fix for OCG: (Task T148076)
- Deploy redundant unified certs (Task T148131)

Category: Incident documentation