GMO GlobalSign Incident Report

Certificates non-compliant with Apple's Certificate Transparency Policy

29th April 2021

www.globalsign.com

Background Details

On the 23rd April 2021 at 16:17 UTC, GlobalSign was informed of certificates issued in non-compliance with Apple's Certificate Transparency policy that came in effect on 21st April 2021.

The affected certificates were issued with 2 Signed Certificate Timestamps (SCT) issued from a CT log, where the updated policy by Apple requires *3 Signed Certificate Timestamps for certificates with a notBefore value greater than or equal to April 21, 2021 and a certificate lifetime greater than 181 to 398 days, causing failed TLS connections.* SCTs are timestamps provided by the Certificate Transparency services upon submitting a certificate to the logs.

Following investigation, the team traced the issue to a failed deployment of the SCT configuration update to the affected availability zone.

The issue was resolved on the 26th of April 2021 15:00 UTC and new certificates with a certificate lifetime greater than 181 to 398 days, are issued with 3 SCTs.

Timeline (all times in UTC, mm-dd-yyyy)

04-23-2021 16:17	First notification of certificates with SCT issues
04-26-2021 10:20	Escalation to Infra Team
04-26-2021 14:33	Infra Team discover issue and start investigating
04-26-2021 14:39	Issue is confirmed
04-26-2021 15:00	Fix deployed to resolve issue
04-26-2021 15:16	Issue confirmed resolved. New certificates issued with correct SCT setting.

Root Cause Analysis

To ensure our services are highly available to customers during and after maintenance windows and upgrades, we have two routes “Route A” and “Route B”.

On 17th March, after validating the configuration change in our staging environment, our engineers released the Certificate Transparency configuration change to production. Configuration changes are pushed to one route and then the other, to provide a quick roll-back mechanism should any service-affecting problems be introduced. The active route at the time was Route A, so the updated configuration should have been deployed to Route B following 24-48 hours of stable service.

However, as we noted when investigating the misconfiguration, route B was not updated with this configuration change. The change was tested to be successfully deployed as all issuance was being performed through route A at the time of the deployment. On 26th April, 15:00 UTC the change was pushed as an emergency update to our Route B to resolve the impact.

On 23rd March some further work was carried out on the Route A CT logging configuration to remediate a communication issue with some older non-sharded CT Logs, however this was resolved within 24 hours so the changes were rolled back and never duplicated to Route B (which would have also pushed the previous update).

Route B was promoted to active status on 25th March as part of an update to the platform binaries, so all traffic for certificates issued after April 21st (Apple’s Certificate Transparency Policy effective date) was being served by Route B.

The Infrastructure team has a monitoring system to notify when the configuration pushed to production differs from that committed to source control. However, during March and April 2021 there have been multiple major platform releases and other patches/updates so this reporting has been full of false positives and the particular configuration file for CT logging was missed.

Preventative Measures

The Infrastructure Team will be investigating improvements to the monitoring of configuration deltas between routes which can cope better with busy periods when there are many differences queued for releases.

They will also be looking to improve their tracking processes to ensure that all follow-up and clean-up actions must have been completed before tickets can be closed.

The Operational Governance team are working closely with Infrastructure to develop further synthetic and real-user monitoring to ensure the correct number of CT logs are included as per the latest compatibility rules from all browsers/root programmes.