WHITE PAPER

When Certificates Expire.

Anatomy of a preventable outage, and how to stop the next one before the handshake fails.

47

DOCUMENT	White Paper
VERSION	1.0
PUBLISHED	July 2026
PUBLISHER	Generator Labs · generatorlabs.com

Every certificate outage has the same postmortem. The certificate was valid. Then, on a date everyone could have known in advance, it was not. Sign-ins failed, APIs threw handshake errors, and an engineer spent an afternoon renewing something a calendar reminder was supposed to catch. Nothing was hacked. A clock ran out.

This is the most predictable outage in infrastructure, and it is about to get much harder to avoid. The maximum lifetime of a TLS certificate is being cut from 398 days to 47 by 2029. The renewal cycle that already trips up the largest engineering teams is about to spin roughly eight times faster.

01

Seven public incidents across seven years. **None** was caused by an attack; every one was caused by a date.

The Outage Nobody Scheduled

Expired certificates do not respect company size or engineering maturity, and the incidents are not slowing down:

2018-12-06	**Ericsson / O2**	Expired certificates in mobile-core software knocked out data for roughly 32 million O2 subscribers in the UK, plus SoftBank in Japan.
2020-02-03	**Microsoft Teams**	Unusable for about three hours worldwide because an authentication certificate was not renewed.
2021-02-15	**Google Voice**	New calls failed for over four hours; Google's own incident report names expired TLS certificates as the cause.
2021-09-30	**Let's Encrypt Root**	The DST Root CA X3 expiry broke connections for Fortinet, Shopify, and countless older clients in a single day.
2023-04-08	**Starlink**	A multi-hour global outage that SpaceX attributed to an expired ground-station certificate.
2024-07-31	**Bank of England**	An expired certificate halted CHAPS, the UK's high-value payment system, for 91 minutes.

2025-11-18	**GitHub**	Every Git operation failed for roughly an hour after an internal service-to-service TLS certificate expired.

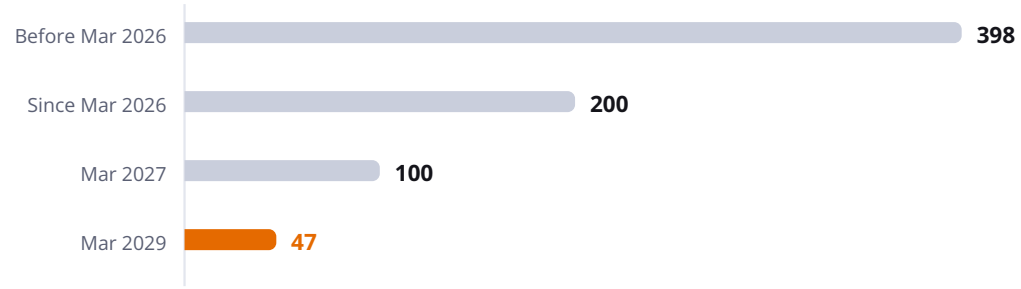
> *If Microsoft, Google, and GitHub can ship a preventable expiry outage, the problem is not competence. It is process.*

02

The Renewal Window Is About to Shrink

CA/Browser Forum ballot SC-081v3, passed April 2025 with Apple, Google, Microsoft, and Mozilla voting yes.

The CA/Browser Forum has set a fixed schedule that phases the maximum TLS certificate lifetime down from 398 days to 47, and the first cut is already in force: certificates issued since March 2026 max out at 200 days.



Maximum TLS certificate validity, days · CA/Browser Forum SC-081v3

By March 2029 a certificate lasts 47 days and its domain validation can be reused for only 10. Every certificate you run will turn over roughly eight times a year.

Manual Renewal Was Already Losing

At 398-day lifetimes, well-resourced teams still missed renewals. At 47 days, one renewal a year becomes eight, for every certificate, on every endpoint, forever. Manual tracking does not scale to that, and the failure mode is a silent outage.

03

Why Renewals Silently Fail

Keyfactor, 2024 PKI & Digital Trust Report. Vendor survey; direction corroborated by

Certificate incidents are not rare. The average organization reported nine in a single year:

Venafi studies in 2019 and 2022.

9	5.3h	32%
CERT INCIDENTS PER YEAR	TO FIND AND FIX EACH	USE A CLM TOOL

- **The certificate you cannot see.** Internal services and wildcard certs reused across hosts fall outside manual tracking. Spotify's 2020 outage, caused by an expired internal certificate, came from exactly this blind spot.
- **The process, not the person.** Renewal often lives in one engineer's head or one spreadsheet. Turnover, vacation, or a reorg removes the human, and the certificate lapses on schedule.
- **Automation gaps.** Only about a third of organizations use a dedicated certificate lifecycle tool.

Automation and Monitoring Are Not the Same Thing

Automated issuance renews the certificates it knows about. It does not tell you when a renewal silently failed, when a cert was deployed outside the pipeline, or when a chain is misconfigured. Monitoring is the independent check that catches what automation misses.

04

Check a single hostname free at **mrdns.com/ssl-check**; continuous monitoring is the product.

What Actually Prevents It

The fix is an outside observer that watches every certificate the way a browser does, on a schedule, and warns you while there is still time to act.

Early Expiry Warnings	Escalating alerts as expiry approaches, so a renewal is never a surprise.
Chain and SAN Validation	Catches broken intermediate chains and missing hostnames, not just the leaf date.
TLS Configuration Checks	Flags weak protocols and configuration issues before they become findings.
Internal Endpoints Included	Service-to-service APIs, admin panels, and queues get the same watch as your public edge. Those are the certificates that fail quietest.

Alerts Where You Work	Email and webhook notifications that reach the people who can act.

Monitoring every endpoint continuously, with alerts and history, is what Certificate Monitoring is for.

KEY TAKEAWAYS

- Expiry is the most predictable failure in infrastructure, and it takes down even the biggest, best-resourced companies.
- Maximum certificate lifetimes drop to 47 days by 2029, making renewals roughly eight times more frequent.
- Renewals fail for process reasons: invisible endpoints, human gaps, and partial automation.
- Continuous, independent monitoring catches the renewal that automation and calendars miss.

05 Sources

1. CA/Browser Forum, Ballot SC-081v3, April 2025: cabforum.org
2. Keyfactor, 2024 PKI and Digital Trust Report: keyfactor.com
3. Ericsson / O2 outage coverage, December 2018: TechCrunch
4. Google Workspace incident report, February 2021: Google
5. Let's Encrypt DST Root CA X3 expiry, September 2021: letsencrypt.org
6. Starlink outage coverage, April 2023: Data Center Dynamics
7. Bank of England annual report (CHAPS outage), 2024: bankofengland.co.uk
8. GitHub incident report, November 2025: github.blog
9. Spotify internal-certificate outage, August 2020: Keyfactor

Catch the Next Expiry Before It Catches You

Generator Labs Certificate Monitoring tracks expiry, chain health, and TLS configuration across every endpoint you run, and alerts you with days to spare instead of minutes. Start free.

portal.generatorlabs.com/signup