

# ProteQC® Research Finds Browser Trust Deadlines Are Already Underway, Offering Early Test of PQC Readiness

---

*Google data shows 13 root certificate deadlines have passed, with 17 more approaching, testing the crypto-agility needed for PQC migration*

LONDON, UNITED KINGDOM, September 1, 2026 /EINPresswire.com/ -- ProteQC, a vendor-neutral post-quantum cryptography (PQC) advisory firm, today released new research (<https://proteqc.com/trust-anchor-migration-support/>) revealing that a major global browser trust transition is already underway, significantly earlier than many organisations may realise.

ProteQC's analysis of [Google's published root certificate data](#) identified 47 Certificate Authority (CA) roots with trust deadlines between July 2025 and September 2027. Of the 13 deadlines that have passed, only one has taken effect for most users. The remaining 12 will take effect with the release of Chrome 153 on September 8. Another 17 deadlines will follow within the next six weeks, including 13 on September 30, 2026.

While these changes are part of routine browser security maintenance, they provide organisations with an immediate test of the same cryptographic agility capabilities they will need for the much larger transition to PQC.

## What This Means in Practice:

The deadlines do not mean websites suddenly stop working. Certificates already issued remain valid until they expire. The impact comes when an organisation renews a certificate that depends solely on an affected root. If the new certificate is no longer trusted by Chrome, visitors may see a full-page security warning instead of the website.

Because certificates are typically renewed within a year, organisations may encounter the issue during their normal renewal cycle rather than on Google's published dates, making the cause harder to identify.

## Three Checks, Ten Minutes:

Organisations can assess their exposure by answering three questions:

1) When does the certificate expire?

- 2) What root is at the end of its certificate chain?
- 3) Does this root appear on the register of those that are expiring?

Most organisations will find they are unaffected. ProteQC is publishing the register and self-checks so they can confirm their exposure directly.

“An organisation that budgeted this as a 2027 programme has already missed thirteen dates, and twelve of them arrive in Chrome on a single day next week,” said Tim D. Williams, Chief Technology Officer of ProteQC. “Google’s 2027 deadline is real, but it is not the one that reaches them first.”

#### Why Root Certificates Matter:

Root certificates form the foundation of trust for secure communications online. Certificate Authorities use them to validate the digital certificates presented by websites and other systems, while browsers maintain lists of the roots they are willing to trust.

The connection to post-quantum migration is direct. As quantum computing advances, organisations will need to replace vulnerable cryptography with quantum-resistant alternatives while identifying where it is used, understanding the systems and services that depend on it, and avoiding operational disruption.

The current browser trust changes are modest by comparison, but they provide a practical preview of the same crypto-agility capabilities organisations will need for post-quantum migration at a much greater scale.

#### ProteQC Finds Exposure Is More Complex Than It Appears:

ProteQC's research found that simply counting certificates associated with roots facing retirement significantly overstates actual exposure. Certificate Authorities frequently use cross-signing, allowing a certificate to reach a trusted root by more than one valid path. A certificate with a second route can continue to work even when one root is retired.

Rather than publish an estimate based on public data that proved unreliable, ProteQC has released a register identifying every affected root and its relevant dates, allowing organisations to assess their own exposure.

“An earlier estimate relied on public data that we ultimately found wasn’t reliable enough, so we withdrew it before publishing,” said Williams. “We’ve published the corrections alongside the research because we believe transparency around the methodology is just as important as the findings.”

#### The Risk Browser Testing May Not Reveal:

Browsers typically update their trusted root certificates automatically, but many other systems do not. Java runtimes, payment terminals, embedded devices and server-to-server integrations may maintain their own trusted root lists, which can become outdated over time. If these systems do not trust the replacement root, the result can be an outright connection failure that disrupts critical integrations without an obvious warning to users.

ProteQC's analysis highlights the gap. A 2022 Java installation contained only eight of the 53 roots that will remain valid, while a current patched build from another supplier contained all of them. Older installations may continue operating because Certificate Authorities provide additional cross-signed certificates, but organisations cannot assume those alternative paths will remain available.

#### A Real-World Dress Rehearsal for Post-Quantum Migration:

The browser trust transition is modest compared with the cryptographic transformation ahead, but the operational questions are similar: Which systems depend on the affected cryptography? Which users, partners and technologies can support the replacement? Where are legacy systems creating hidden dependencies? How quickly can an organisation make a cryptographic change when someone else controls the deadline?

"An organisation that can answer those questions for root certificate changes in 2026 and 2027 will be better positioned to answer them for post-quantum cryptography," said BJ Miller, Chief Executive Officer of ProteQC. "One that cannot may discover those gaps during a much larger and more complex migration. This is an opportunity to identify them now, while the stakes are considerably lower." □□

#### ProteQC Makes Research and Tools Freely Available:

ProteQC is publishing its full deadline register, research methodology and correction log free of charge with no registration required. The resources include every affected root, its deadline and effective date, along with commands organisations can use to determine which certificates their own systems present and trust. □□A comparison of trusted root lists across four Java builds is also available, along with the underlying data and transcript of a controlled demonstration.

LINK TO RESEARCH AND FREE RESOURCES - <https://proteqc.com/trust-anchor-migration-support/>

Organisations looking to better understand their exposure or assess their readiness can also contact ProteQC at [info@proteqc.com](mailto:info@proteqc.com) for guidance on where to start.

To learn more about ProteQC and the ProteQC PQC Lifecycle Framework™, visit <https://proteqc.com>.

Ana Perez Quiles  
ProteQC  
2038355326 ext.  
[email us here](#)

---

This press release can be viewed online at: <https://www.einpresswire.com/article/938660056>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.