Quad9 Incident Post-Mortem

2026-05-08 quad9.net authoritative nameservers disruption

version 2, 2026-05-11

Contents

Summary

On May 8th, 2026, Quad9's primary zone, "`quad9.net`", experienced a roughly 40-minute outage due to a failed validation step between our primary hidden authoritative nameservers and public anycast nameservers hosted by PCH.

The outage was caused by legacy configuration that was not correctly documented and was inadvertently modified during recent maintenance.

Timeline

All times privided in UTC unless explicitly mentioned otherwise.

Timestamp	Event
2026-05-08 15:50 UTC	First zone failures logged
2026-05-08 16:03 UTC	Incident response work begins
2026-05-08 16:11 UTC	Incident announced on Quad9 status page
2026-05-08 16:31 UTC	Root cause identified and solution implemented
2026-05-08 16:45 UTC	Full recovery confirmed
2026-05-08 17:18 UTC	Incident resolved

Incident

Quad9 experienced outage intervals up to about 40 minutes for our primary zone "`quad9.net`" due to a failed validation step between our primary hidden authoritative servers and PCH's anycast network, which we use for externally-facing DNS authoritative services.

The root cause was determined to be due to legacy exchanged configurations between PCH and Quad9 which were not documented clearly, and recent maintenance changes caused a failure in importing the zones to the authoritative pipeline.

The first log record of zone failures being evident was computed to be sometime after 2026-05-08 15:50 UTC. Quad9 systems teams began resolution work at 16:03 UTC and coordinated with PCH for a solution that was implemented at 16:31 UTC when the zone data was restored. Full recovery was observed at 16:45 UTC.

Impact

Users utilizing 9.9.9.9 and other IP-based service addresses for DNS resolution were not impacted during this event, except for lookups to hosts under quad9.net. Other zones and recursive services remained operational.

Users attempting to use DNS client encryption with our named records of "`dns.quad9.net`" or other service names under `quad9.net` would not have been able to create new connections, as those queries would have been sent to

client local resolvers not operated by Quad9. Existing encrypted sessions would have remained operational until re-establishment due to network change or timeout of TTL for the `dns.quad9.net` hostname.

Users transitioning from IP-address based sessions and using DDR (RFC9462) to upgrade to encryption using name-based addresses may have experienced no issues as those queries would have been answered by Quad9's recursive resolvers and include IP address hints as part of the response.

Users attempting to use `www.quad9.net` would have been unable to reach that service for the interval of the outage, and our inbound mail system was also unreachable in that interval.

Depending on timing of lookups by outside recursive resolvers to the names in the `quad9.net` zone, the varying expiration of TTLs may have meant a significantly shorter outage window.

Recovery

Incident response team coordinated closely with PCH to establish the root issue and implement a fix. Once the faulty configuration was identified, the fix was deployed, and within a short time full recovery was observed.

Recommendations

Quad9 is in the process of revising our authoritative nameserver set, and has planned to shift to a more instrumented configuration in the next few weeks. This fault was unrelated to that already-planned transfer.

The upcoming changes will lead to a better architectural solution which we hope will reduce or eliminate this particular fault path.