Post-Mortem: Premium DNS Outage, September 2-3, 2026

Published: 3 September 2026 | Status: Resolved

On September 2-3, 2026, domains using Openprovider's Premium DNS product experienced a DNS resolution outage caused by a failure at our upstream provider, Sectigo. For affected domains, websites, email delivery, and other DNS-dependent services were unreachable for a significant part of this period. The issue was fully outside Openprovider's infrastructure, but these are our customers and our product, and we take full ownership of the impact and of how we communicated during the incident.

We know this is not the first Sectigo-related Premium DNS incident this year, and we understand how damaging repeated DNS outages are for you and your customers. This post explains what happened, what we did, where we fell short, and the concrete steps we are taking, including a migration to a new Premium DNS provider that is already in progress.

What happened

Sectigo, the vendor operating the nameservers behind our Premium DNS product (ns1-ns4.sectigoweb.com), migrated their own domain infrastructure to a new platform and failed to carry over the address records for their nameservers. As a result, their authoritative DNS could no longer resolve their own nameserver hostnames, and DNS queries for zones hosted on the service began failing with SERVFAIL errors.

Because DNS sits underneath everything else, the impact for affected domains was broad: websites (A, AAAA, CNAME records), email delivery (MX), email authentication (SPF, DKIM, DMARC), and certificate validation (CAA) were all affected until resolution was restored.

Domains using Openprovider's own nameservers were not affected at any point.

Timeline (all times CEST)

September 2

- ~15:22, first customer reports received; our support team identified the pattern and began investigating within 20 minutes
- ~16:15, root cause identified by our engineers: Sectigo's nameserver address records had been orphaned during their own platform migration

- ~16:15-16:29, incident published on statuspage.openprovider.eu and Sectigo's emergency contacts engaged
- Afternoon and evening, we escalated continuously through every available channel at Sectigo, by phone, email, and direct executive contact, including members of our leadership team personally reaching Sectigo's Director of Global Sales Engineering
- Throughout, our support team replied to every incoming ticket and worked directly with the most heavily affected reseller accounts

September 3

- ~02:21, Sectigo confirmed a configuration fix had been deployed
- ~04:35, our support team updated all open tickets and confirmed the majority of Premium DNS zones were resolving again
- Morning, recovery reconfirmed, status page updated, and every customer who had contacted us received a direct reply

What we did well

Our team detected and diagnosed the issue quickly, identifying the exact root cause on Sectigo's side within an hour, faster than the vendor itself communicated it. We kept replying to every ticket even before a fix existed, pursued the vendor relentlessly through multiple escalation paths when their standard support channel stalled, and confirmed with every affected customer after restoration.

Where we fell short

We believe in being transparent about our own performance, not just our vendor's.

Our first public status update was a bit slow. Our internal standard is a public status update within 15 minutes of a customer-affecting incident. The first Statuspage post went live roughly an hour after the first customer report. That is not good enough, and we have reinforced the process and are automating the reminder so the clock is visible from the moment an incident is opened.

We had no bulk mitigation available. The available workaround, recreating a DNS zone on Openprovider's own nameservers and repointing the domain, only worked domain by domain. For resellers managing large portfolios, that does not scale, and we could not offer a scripted alternative during the incident. We are building a bulk mitigation path and adding engineering capacity to our incident on-call rotation so that a workaround like this can be built while an incident is live.

This was a repeat vendor incident. Sectigo's Premium DNS service also suffered a significant outage earlier this year. A single outage can happen to any provider; a repeated pattern requires a structural answer, which brings us to the most important part of this post.

What we are changing

1. We are replacing Sectigo as our Premium DNS provider. A migration to a new premium DNS platform with a stronger reliability track record was already underway before this incident. The core engineering integration is in an advanced stage, and following this outage we are prioritizing a committed cutover timeline. Existing Premium DNS zones will be migrated for you; we will communicate the schedule and any actions needed (in most cases, none) well in advance.

2. Faster, more disciplined status communication. The 15-minute first-update and 4-hour cadence rules are being reinforced with automated reminders tied to incident creation, and we have removed internal ambiguity about posting before full details are confirmed. An early "we are investigating" post is always better than silence.

3. Bulk mitigation tooling for resellers. We are defining a scripted bulk path to move affected zones onto Openprovider's own nameservers during a vendor outage, so portfolio customers are no longer dependent on per-domain manual work.

4. On-call engineering for vendor incidents. A developer is being added to the incident rotation so that mitigations can be built in real time, not just identified.

5. Structural vendor review. We are introducing an annual supplier review covering service quality, support responsiveness, communication, and financial sustainability, and even after the migration we will maintain a fallback plan so no single DNS vendor is ever again a single point of failure.

To our customers

Several of you quoted our own uptime commitment back to us during this incident. You were right to. Premium DNS exists precisely so that your domains stay online, and twice this year a vendor failure has broken that promise. The migration described above is the structural fix, and we will report on its progress publicly.

If any of your domains are still experiencing issues, or if you want to discuss moving zones to Openprovider's own nameservers in the meantime, please contact our support team, and thank you for your patience and directness throughout this incident.