Incident report: VKMS service interruption, October 26–27, 2026

Prepared by: VKMS Cloud Operations

Status: Resolved. Permanent fix in place since October 30, 2026.

Times are US Central (CDT), with UTC in brackets.

Summary

From 4:45 pm on Monday, October 26 until 7:20 am on Tuesday, October 27, VKMS (version 12) sites were unavailable, about 14½ hours. Users saw a "502 Bad Gateway" page instead of their site.

The cause was a change in the list of certificate authorities that Microsoft trusts, combined with a security setting at the entrance to our platform that accepted only one of them. No customer data was lost, changed or exposed.

We restored service on the morning of October 27. On October 30 we removed the setting that made us vulnerable to this kind of change, so the same event can't interrupt service again.

Impact

- **Who:** all customers on VKMS version 12, production and staging sites.
- **What users saw:** a "502 Bad Gateway" error page instead of their site.
- **When:** October 26, 4:45 pm (21:45 UTC) to October 27, 7:20 am (12:20 UTC).
- **Data:** none lost, changed or exposed. The applications and databases kept running the whole time. The interruption happened at the entrance to the platform, before any request reached the application.

What happened

Some background. When a browser connects to a website, the site shows a digital certificate, which works much like an ID card. A certificate is trusted because it was issued, directly or through a chain of other certificates, by a recognized certificate authority. Microsoft, Google, Apple and others each keep a list of the authorities they trust, and they update those lists automatically.

How our platform checks certificates. All traffic to VKMS sites passes through a secure gateway, which works like the front desk of a building. It checks each of our application servers' certificates before passing traffic on. That front desk was set to accept certificates from **one** authority only, an older authority that had been part of our setup for years.

The change. Microsoft updated the list of authorities that Windows trusts, and removed that older authority from it. The updated list is dated October 23. The change appears to be part of the industry's

response to a security incident at another certificate authority, disclosed in mid-October, which involved certificates linked to this older authority. Microsoft made the change automatically and without notice.

The effect. Our application servers run on Windows, in Microsoft Azure. Once they adopted the updated list, they began presenting their certificates through a newer, fully trusted authority instead of the old one. Our certificate itself didn't change and remained valid throughout. But the front desk still accepted only the old authority, so from 4:40 pm on October 26 it turned every site away, one after another.

In short, the certificate stayed valid and the servers stayed healthy. Every site went down because the gateway trusted only one authority.

How we restored service

On the morning of October 27 our team traced the errors to the gateway's certificate check.

- **7:17 am:** after confirming the fix on several sites, we updated the gateway to accept the newer authority.
- **7:20 am:** every site was back and verified.

What we changed so it can't happen again

The root cause is removed. On October 30 we changed the gateway so it no longer depends on any single certificate authority. It now accepts any authority on Microsoft's trusted list, the way a web browser trusts any recognized authority rather than one hand-picked one. When an authority is retired in the future, the gateway follows the updated list automatically instead of blocking traffic.

How we made the change safely:

- **3:32 am:** applied first to one test site, which we watched for 15 minutes.
- **4:20 am:** applied to all sites, outside business hours, in an update that took under a minute.
- **Through the morning:** we checked every site again at regular intervals. All sites stayed available, with error levels the same as on a normal day.

Our next-generation platform (VKMS version 14) uses a different design, which already follows Microsoft's trusted list and has no such restriction.

Closing

We're sorry for the disruption this caused you and your teams. The setting that turned a routine industry change into an outage has been removed, and it has been verified in production. No action is needed on your side. If you have any questions about this report, please contact your VKMS account representative.