VTEX

The Enterprise Digital Commerce Platform

Incident Report

Feb 9, 2024 : Degraded performance in Portal Application

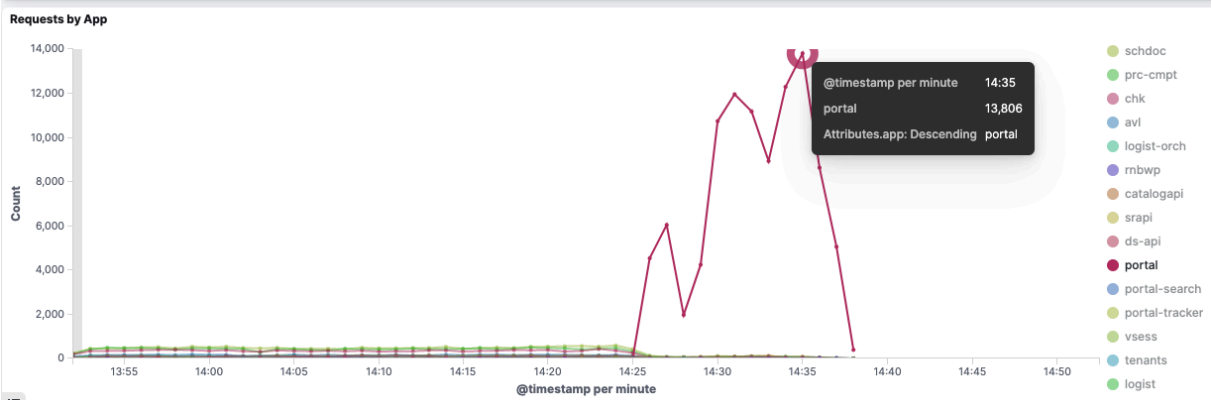
Status Page URL	https://status.vtex.com/incidents/01HP75WG0C1Z5THDKZCYFRK0A6
Impacted accounts	All stores
Duration	16 minutes (14:26 to 14:42 UTC)
Availability	Stores were unavailable facing 5xx errors while navigating.

Summary

On Feb 09, 2024, from 14:26 to 14:42 UTC, shoppers experienced 5xx errors while navigating and fulfilling orders. The occurrence of this symptom was related to an unexpected increase in requests to the Portal Application, which affected our global sales flow and storefront navigation for 16 minutes.

The incident was triggered by a surge in requests for one account, over 10 times the anticipated volume, indicative of a targeted attack (Image 1). As a mitigation we identified possible attackers and ensured that the environment was scaling properly. As soon as the environment scaled and the requests normalized the operation returned to normal.

Image 1 – Requests on Balancer



Platform traffic was approx 10 times higher from 14:25 to 14:37

Symptoms

The portal application experienced a high error rate due to an influx of non-organic requests targeting a single account indicative of a targeted attack. Shoppers experienced 5xx errors while navigating and fulfilling orders. This symptom could be observed in some navigation sessions happening between 14:26 to 14:42 UTC.

Timeline

[2024-02-09 14:26 UTC]	Our alarms were triggered alerting our incident response team of a rapid increase in error rates in our platform. Automated self-healing mechanisms started scaling our infrastructure automatically according to the new level of requests.
[2024-02-09 14:28 UTC]	Our incident response team started investigating the issue.
[2024-02-09 14:37 UTC]	We identified the pattern of aggressors and initiated mitigation to prevent these attacks.

[2024-02-09 14:42 UTC]	The requests have returned to regular rates. Platform behavior was reestablished. Our team continued monitoring and investigating to prevent the attack from affecting us again.
[2024-02-09 16:59 UTC]	We completed a full analysis.
[2024-02-09 16:02 UTC]	We declared the incident resolved.

Mitigation strategy

Several response actions were taken to mitigate the impact and resolve the issue. Here is a summary of the key response actions:

- Ensure that the self-healing mechanism was scaling the infrastructure correctly.
- Identify and block the traffic that was affecting the platform.

Follow-up actions: Preventing future failures

As a follow-up to this incident, we are working to ensure that this type of request and navigation pattern is blocked at the very edge, preventing it from reaching our infrastructure in the future.