Summary of QuickLaunch Service Event
August 25th, 2025

QuickLaunch wants to provide you with additional information about the service disruption that occurred on **August 25, 2025**, which impacted authentication services through the Password Manager module.

Summary

On August 25, 2025, QuickLaunch experienced a service disruption affecting the Password Manager module. The disruption began at 11:35 AM ET, preventing some users at multiple institutions from authenticating successfully and resulting in error messages during login.

Our engineering team immediately investigated and identified the issue as isolated to the Password Manager module. Customers were notified of the incident at 1:00 PM ET. By 1:10 PM ET, partial service was restored following infrastructure scaling and configuration tuning. Full-service stability was confirmed by 1:53 PM ET, and a final restoration notice was issued to all customers at 2:55 PM ET.

Date	Time (EST)	Chronological Issue Summary - Root Cause Analysis
Monday, August 25, 2025	11:35 AM	Issue detected by QuickLaunch team following client reports.
	11:40 AM	Investigation started by Engineering team.
	11:55 AM	Alerts confirmed disruption within the Password Manager module.
	1:00 PM	Service disruption notification sent to customers. Infrastructure scaled (max_connections, threadpool).
	1:10 PM	Partial service restoration achieved.
	1:35 PM	Monitoring confirmed traffic normalization.
	1:53 PM	Engineering confirmed stable restoration.
	2:55 PM	Service restoration notice sent to customers.

Root Cause Analysis

QuickLaunch would like to provide additional context regarding the service disruption that occurred on **August 25, 2025**, affecting the Password Manager module. This disruption impacted authentication services for users at multiple institutions, preventing some from being able to log in successfully and causing error messages to appear during the login process.

The disruption began at 11:35 AM ET when QuickLaunch detected unusual behavior and began receiving reports from clients. Our engineering team immediately initiated an investigation and confirmed that the issue was isolated to the Password Manager module. While initial remediation efforts were underway, customers were notified of the service disruption at 1:00 PM ET. By scaling up infrastructure capacity and tuning configuration settings, QuickLaunch was able to partially restore service within ten minutes, with stability confirmed by 1:53 PM ET. A final service restoration notice was issued to all customers by 2:55 PM ET.

RCA:

The service disruption was the result of **Apache thread pool exhaustion** under heavy load conditions. As new login requests were submitted, Apache’s worker threads became saturated, which led to a backlog of queued requests and eventual timeouts. This caused a cascading effect across dependent services, including authentication, database operations, and APIs, all of which rely on timely responses from Apache.

Once the worker threads were fully consumed, Apache could no longer process new requests, which rendered the Password Manager service unresponsive. This behavior is consistent with saturation failure modes in web servers operating at or near capacity. While QuickLaunch systems are designed with fault tolerance in mind, the sudden exhaustion of thread pools meant that end users attempting to log in during this window were unable to complete the process.

Corrective Actions:

QuickLaunch engineers took immediate action to mitigate the impact and restore services.

Steps included:

- Restarting affected services.
- Scaling pods within the cluster and provisioning additional compute resources.
- Tuning Apache configuration parameters in real time (e.g., increasing maximum connections and thread pool allocations).

By executing these measures, authentication traffic began flowing normally within minutes, with stability achieved by 1:53 PM ET.

To prevent recurrence, QuickLaunch has implemented both short-term fixes and long-term improvements:

- Proactive Monitoring: Enhanced health checks now monitor thread pool utilization in real time, enabling earlier detection of saturation risks.
- Capacity Hardening: Infrastructure and capacity across key modules have been increased (with selective over-provisioning) to absorb unexpected traffic spikes.
- Performance Reviews: An increase in regular capacity and performance stress testing have been scheduled to anticipate demand surges and optimize system resilience.

QuickLaunch Service Impact Summary

The intermittent availability and service disruption of the QuickLaunch Services affected the ability of certain users to successfully login and access their systems.

Restoration Plan Summary

Phase 1: Immediate issue remediation Completed

Phase 2: Service Verification Completed

Phase 3: Post-Incident Review In Progress

Phase 4: Proactive Monitoring Enhancements In Progress

Phase 5: Updated capacity and performance reviews Capacity Increased, On-going Reviews In Progress

In Closing

QuickLaunch recognizes the critical importance of uninterrupted authentication services for our customers and their end users. While our systems are built with fault-tolerant principles, the sudden exhaustion of Apache’s worker threads temporarily impacted end-user login experiences. We also want to emphasize that this disruption was **not the result of a security breach or malicious attack**. No customer data was corrupted, exposed, or compromised during the event.

QuickLaunch will continue to take every possible step to strengthen the resilience and scalability of our platform. Our teams remain committed to delivering secure, reliable, and high-performing services for the institutions we serve. The corrective measures now in place significantly reduce the likelihood of recurrence and strengthen our overall service reliability.