## Recent Incidents

August 23, Tue

### QuickLaunch IDP8 - Investigating Service Disruption Alarms

Resolved in 7 hours

Affected Service: Single Sign-On & Identity Provider | Password Manager with MFA | Multifactor Authentication

3:58, Aug 23 EDT

**Resolved**

3:45pm ET

**Solution #3 - Denial of Service Patch Released for Restoring Login Services** -

Major Update: QuickLaunch has deployed a patch for restoring login services (8.12.4) to production. This patch restores login services without password management and AMFA services as an emergency workaround. This patch will not call custom CSS pages and hence for customers with a customized login/post-login page, please be advised that you will see a more standard login page experience.

Login services for affected customers should be restored, however there may be customers with custom configurations that will require scheduled calls with the QuickLaunch engineers.

**Solution #1 Denial of Service Workaround Update**

This solution continues to being deployed for customers. Customers who have deployed this solution have been able to restore login services for end users.

Status Updates: We have received feedback that customers are not getting updates. Bookmark this page for status updates. https://quicklaunch.io/outage-status/

Thanks-QuickLaunch Support

3:43, Aug 23 EDT

**Fixing**

2:15pm ET -

**Solution #3 - Denial of Service Patch Developed for Restoring Login Services**

QuickLaunch has developed a patch for restoring login services without password management and AMFA. This patch is being tested. QuickLaunch currently expects to complete testing by approximately 3:45pm ET. If tests are successful, we will send an update once the patch is scheduled to be released in production. Once released, this will restore login services for all affected customers.

**Solution #1 - Denial of Service Workaround Update**

This solution continues to being deployed for customers. Customers who have deployed this solution have been able to restore login services for end users.

Thanks-QuickLaunch Support

3:10, Aug 23 EDT

**Fixing**

**Solution #1 Major Update - Denial of Service Workaround Successfully Deployed:**

QuickLaunch has tested solution #1 to workaround the denial of service attack on password management services successfully. QuickLaunch setup a SAML2.0 bridge for login services that bypasses the affected password manager services as well as AMFA services. In test, the login services successfully transact logins. The QuickLaunch team has applied this solution to two customers and this is running successfully in production. Our team will start reaching outbound to customers to queue up this option.

**Solution #2 Update - AWS:**

In addition to this, QuickLaunch architects are still working with AWS on resolving the denial of service attack. We have not yet received an ETA for this resolution.

Thanks-QuickLaunch Support

12:57, Aug 23 EDT

**Fixing**

**What is the this outage, technically?**
Denial of Service on QuickLaunch Password Manager Services. This DOS attack on the public URL - Password.QuickLaunch.io is generating password reset by what seems to be a bot that is using one of the customer domains to make password reset calls. The flood of these password reset calls which started at approximately Tuesday, 8:15 AM ET are creating performance issues on Password Manager services and as the password reset calls pool, the logs show that the Login services become non-performant and unavailable as a result. Due to QuickLaunch's architecture setup on multi-node and auto-scaling, the Login service will "spin" for end users as Login requests continue to increase and pool.
Snippet of Denial of Service logs:
Aug 23 13:01:36 QL8-PROD-PASSWORDMANAGER1 kernel: [ 913.933432] TCP: request_sock_TCP: Possible SYN flooding on port 8080. Sending cookies. Check SNMP counters.

**What is the impact of this outage?**
QuickLaunch Password manager is tightly coupled with identity infrastructure. As the Password manager API is under attack it has also impacted login process to become sluggish to the extent of being unavailable most times.

**Are all institutions affected or just us, or something in between?**
All schools using Password Manager v8.12 are affected.

**What is QuickLaunch doing at this time? what is the recommended plan of action?**
QuickLaunch is pursuing a two pronged attack at this point in time:
a. QuickLaunch Network engineers and AWS support are on a call to address this denial of service attack on the QuickLaunch Password Manager services - Password.QuickLaunch.IO.
b. QuickLaunch architects are setting up and testing emergency work arounds to enable Login services without calling Password Management services.

**Could you not block the client domain that is using the bot to make a password reset call?**
We cannot as we are a multi-tenant platform and request comes in from worldwide locations.

**Can we use the system without using password manager?**
Yes, This is part of work around solution till the time we are able to resolve Denial of Service attack.

**Is the attack coming from a specific location and IP address?**
The attack seems to be coming from different locations and IP addresses.

**How can we receive current updates to keep our community abreast?**
You can click on this link for most recent updates - https://quicklaunch.io/outage-status/. Additionally, you can also reach out to your QuickLaunch Customer Success managers and Support teams via email, ticket, and teams chat. QuickLaunch customer representatives are outreaching all affected clients individually too.

Thanks-QuickLaunch Support

10:35, Aug 23 EDT

**Fixing**

9:15am ET - Denial of Service on QuickLaunch Password Manager Services: QuickLaunch engineers isolated Password Manager services to its own multi-node architecture. Engineers identified in the logs of the Password Manager service a denial of service attack on the public URL - Password.QuickLaunch.io. The denial of service attack is generating password reset by what seems to be a bot that is using one of the customer domains to make password reset calls.

The flood of these password reset calls which started at approximately 8:15am ET are creating performance issues on Password Manager services and as the password reset calls pool, the logs show that the Login services become non-performant and unavailable. Due to QuickLaunch's architecture setup on multi-node and auto-scaling, the Login service will "spin" for end users as Login requests continue to increase and pool.

QuickLaunch Network engineers and AWS support are on a call to address this denial of service attack on the QuickLaunch Password Manager services - Password.QuickLaunch.IO.

Emergency Solutions: In parallel, QuickLaunch architects are setting up and testing emergency work arounds to enable Login services without calling Password Management services. One solution includes temporarily disabling Password Manager services until such time as the denial of service attack is resolved so that customers and end users can login and access services during this critical time.

Thanks-QuickLaunch Support

08:56, Aug 23 EDT

**Investigating**

8:15am - Our monitoring systems have received alerts of service degradation on QuickLaunch Password Manager and AMFA services. Currently the engineers are checking if these services are causing delays and timeouts in Login service load and processing. Login services may be intermittently available while engineers debug and troubleshoot.

Thanks-QuickLaunch Support