

# LastPass Guide

*13 December 2023*

LastPass...|

## Incident 1 – Additional details of the attack

### Incident 1 – Additional details of the attack

On August 12, 2022, our security team was alerted to suspicious activity in a cloud-based development environment used for on-demand and pre-production development, integration, testing, and validation. We immediately launched an investigation and triaged the event to understand its scope.

Over the following 24 hours, our investigation revealed patterns of behavior and access inconsistent with the LastPass software engineering employee who was shown to have accessed these development resources. It soon became evident that the software engineer's corporate laptop had been compromised to allow access to resources to which the engineer was legitimately granted access.

On August 13, 2022, we engaged Mandiant to assist with incident response activities. As part of our investigation, we determined that the timeline of threat actor activity began on August 8, 2022 and lasted until August 12, 2022.

Due to anti-forensic activity performed by the threat actor, as well as a scheduled operating system upgrade during the incident timeframe, which overwrote logs and system artifacts, the initial threat vector that the threat actor used to gain access to the software engineer's machine is not known at this time. The laptop was configured with a standard corporate build of development applications, utilities, and security controls. These included an Endpoint Detection Response (EDR) agent, which was tampered with and was not triggered during the initial activity.

The threat actor used third-party VPN services to obfuscate the origin of their activity when accessing the cloud-based development environment and used its access to impersonate the software engineer. Using this approach, they were able to "tailgate" into the on-demand development environment via our corporate VPN, as well as a dedicated connection to the cloud-based development environment. They did so by relying upon the software engineer's successful authentication with domain credentials and MFA. No privilege escalation was identified or required.

## Incident 1 – Additional details of the attack

The threat actor leveraged access to this development environment and, in turn, accessed technical documentation and LastPass source code to exfiltrate 14 of approximately 200 source code repositories of various components of the LastPass service.

Some of these source code repositories included cleartext embedded credentials, stored digital certificates related to our development environments, and some encrypted credentials used for production capabilities such as backup. These encrypted credentials require a separate decryption key which was not available to the software engineer or the threat actor during this incident.

No customer data or vault data was taken during this incident, as there is no customer or vault data in the development environment. It is also important to note that the cloud-based development and on-premises production data center environments are physically and logically separated.

Our investigation concluded with the remediation items described below. We are confident that we successfully contained and eradicated any access to, and potential persistence in, the affected development environment and engineer's laptop, both of which were removed completely from service.

As we progressed through incident response and as part of containment, eradication, and recovery, we took the following actions:


- Our security team took possession of the affected software engineer's corporate laptop, performed forensic analysis, replaced the machine with a new device running a different operating system, and deleted and replaced all existing domain credentials. Furthermore, the security team worked with the engineer to assist in hardening their home network and personal resources.
- We deployed an additional managed EDR solution configured to augment existing security controls of software engineers' laptops.
- We completed tuning of additional preventative and detective security controls on company laptops and enabled additional logging.
- We deployed a Secure Access Service Edge (SASE) solution to manage direct split-tunneled Internet access and began the replacement of VPN access with a Zero Trust Network Access (ZTNA) solution.

## Incident 1 – Additional details of the attack

- We purchased new hardware authentication devices for software and platform engineering development use cases, including authentication, authorization, and code safety.
- We rotated all LastPass credentials, certificates, and secrets known to have been obtained by the threat actor.
- Our security operations team updated the upstream managed Web Application Firewall (WAF) service and initiated heightened monitoring for anomalous activity.
- We enabled additional Workload EDR monitoring in development and production and deployed additional container introspection capabilities.
- We deployed a market-leading Cloud Security Posture Management (CSPM) platform to provide additional attack surface visibility, asset, and vulnerability management across the cloud platform.
- To remove any potential for persistence and to ensure containment and eradication, we disabled and removed access to the development environment, preserved artifacts for evidence, and ultimately destroyed the environment. We then recreated the entire environment from scratch over a six-week period.
- We deployed updated Kubernetes and Docker configurations in the new development environment, along with additional logging and alerting focused on Cloud Identity and Access Management (IAM) role restrictions.
- We restricted and removed access of engineers/developers to the underlying cloud platform.
- We deployed “canaries” within our production and development environments to augment our intrusion deception and detection capabilities.
- We enabled additional logging in both development and the production environments.
- We engaged a well-known third party to assist with targeted, proactive threat hunting in production environments, in addition to continued engagement with Mandiant for incident response and forensics.

We declared the incident closed and began focusing on additional remediation efforts to strengthen our environment’s security posture. We also resumed building net new development and production environments to facilitate the completion of our corporate separation.

## Incident 1 – Additional details of the attack

 **Note:** To read the complete update on the security incident from our CEO, Karim Toubba, [visit the LastPass blog](#).