Notice of Recent Security Incident

Update as of Thursday, September 15, 2022

To All LastPass Customers,

On August 25th, 2022, we notified you about a security incident that was limited to the LastPass Development environment in which some of our source code and technical information was taken. I wanted to update you on the conclusion of our investigation to provide transparency and peace-of-mind to our consumer and business communities.

We have completed the investigation and forensics process in partnership with Mandiant. Our investigation revealed that the threat actor's activity was limited to a four-day period in August 2022. During this timeframe, the LastPass security team detected the threat actor's activity and then contained the incident. There is no evidence of any threat actor activity beyond the established timeline. We can also confirm that there is no evidence that this incident involved any access to customer data or encrypted password vaults.

Our investigation determined that the threat actor gained access to the Development environment using a developer's compromised endpoint. While the method used for the initial endpoint compromise is inconclusive, the threat actor utilized their persistent access to impersonate the developer once the developer had successfully authenticated using multi-factor authentication.

Although the threat actor was able to access the Development environment, our system design and controls prevented the threat actor from accessing any customer data or encrypted password vaults.

Firstly, the LastPass Development environment is physically separated from, and has no direct connectivity to, our Production environment. Secondly the Development environment does not contain any customer data or encrypted vaults. Thirdly, LastPass does not have any access to the master passwords of our customers' vaults – without the master password, it is not possible for anyone other than the owner of a vault to decrypt vault data as part of our Zero Knowledge security model.

In order to validate code integrity, we conducted an analysis of our source code and production builds and confirm that we see no evidence of attempts of code-poisoning or malicious code injection. Developers do not have the ability to push source code from the Development environment into Production. This capability is limited to a separate Build Release team and can only happen after the completion of rigorous code review, testing, and validation processes.

As part of our risk management program, we have also partnered with a leading cyber security firm to further enhance our existing source code safety practices which includes secure software development life cycle processes, threat modeling, vulnerability management and bug bounty programs.

Further, we have deployed enhanced security controls including additional endpoint security controls and monitoring. We have also deployed additional threat intelligence capabilities as well as enhanced detection and prevention technologies in both our Development and Production environments.

We recognize that security incidents of any sort are unsettling but want to assure you that your personal data and passwords are safe in our care.

Thank you for your continued trust and support.

Karim Toubba

CEO LastPass