Karim Toubba
CEO, LastPass

More Articles

Topics

Product Updates

November 30, 2022 | By Karim Toubba

Notice of Recent Security Incident

Update as of Wednesday, November 30, 2022

To All LastPass Customers,

In keeping with our commitment to transparency, I wanted to inform you of a security incident that our team is currently investigating.

We recently detected unusual activity within a third-party cloud storage service, which is currently shared by both LastPass and its affiliate, GoTo. We immediately launched an investigation, engaged Mandiant, a leading security firm, and alerted law enforcement.

We have determined that an unauthorized party, using information obtained in the August 2022 incident, was able to gain access to certain elements of our customers' information. Our customers' passwords remain safely encrypted due to LastPass's Zero Knowledge architecture.

We are working diligently to understand the scope of the incident and identify what specific information has been accessed. In the meantime, we can confirm that LastPass products and services remain fully functional. As always, we recommend that you follow our best practices around setup and configuration of LastPass, which can be found here.

As part of our efforts, we continue to deploy enhanced security measures and monitoring capabilities across our infrastructure to help detect and prevent further threat actor activity.

We thank you for your patience while we work through our investigation. As is our practice, we will continue to provide updates as we learn more.

Karim Toubba

LastPass CEO

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

Original post from August 25, 2022

To All LastPass Customers,

I want to inform you of a development that we feel is important for us to share with our LastPass business and consumer community.

Two weeks ago, we detected some unusual activity within portions of the LastPass development environment. After initiating an immediate investigation, we have seen no evidence that this incident involved any access to customer data or encrypted password vaults.

We have determined that an unauthorized party gained access to portions of the LastPass development environment through a single compromised developer account and took portions of source code and some proprietary LastPass technical information. Our products and services are operating normally.

In response to the incident, we have deployed containment and mitigation measures, and engaged a leading cybersecurity and forensics firm. While our investigation is ongoing, we have achieved a state of containment, implemented additional enhanced security measures, and see no further evidence of unauthorized activity.

Based on what we have learned and implemented, we are evaluating further mitigation techniques to strengthen our environment. We have included a brief FAQ below of what we anticipate will be the most pressing initial questions and concerns from you. We will continue to update you with the transparency you deserve.

Thank you for your patience, understanding and support.

Karim Toubba

CEO LastPass

FAQs

1. Has my Master password or the Master Password of my users been compromised?

No. This incident did not compromise your Master Password. We never store or have knowledge of your Master Password. We utilize an industry standard Zero Knowledge architecture that ensures LastPass can never know or gain access to our customers' Master Password. You can read about the technical implementation of Zero Knowledge here.

2. Has any data within my vault or my users' vaults been compromised?

No. This incident occurred in our development environment. Our investigation has shown no evidence of any unauthorized access to encrypted vault data. Our zero knowledge model ensures that only the customer has access to decrypt vault data.

3. Has any of my personal information or the personal information of my users been compromised?

No. Our investigation has shown no evidence of any unauthorized access to customer data in our production environment.

4. What should I do to protect myself and my vault data?

At this time, we don't recommend any action on behalf of our users or administrators. As always, we recommend that you follow our best practices around setup and configuration of LastPass which can be found here.

5. How can I get more information?

We will continue to update our customers with the transparency they deserve.