March 1, 2023 | By Karim Toubba

Security Incident Update and Recommended Actions

To Our LastPass Customers–

I want to share with you an important update about the security incident we disclosed on December 22, 2022. We have now completed an exhaustive investigation and have not seen any threat-actor activity since October 26, 2022.

During the course of our investigation, we have learned a great deal more about what happened and are sharing new findings today. Over the same period, we invested a significant amount of time and effort hardening our security while improving overall security operations. In today's update, I'll review those measures and highlight additional security steps that we are taking.

This update is structured as follows:

- **What happened and what actions did we take?**
- **What data was accessed?**
- **What actions should you take to protect yourself or your business?**
- **What we have done to secure LastPass**
- **What you can expect from us**

We are privileged to serve millions of users and more than 100,000 businesses, and we want to ensure that all of our customers have the information they need to answer their questions. Given the volume of information we are sharing today, we have structured this update with summaries that include embedded links to provide more detailed information on each topic.

We have heard and taken seriously the feedback that we should have communicated more frequently and comprehensively throughout this process. The length of the investigation left us with difficult trade-offs to make in that regard, but we understand and regret the frustration that our initial communications caused for both the businesses and consumers who rely on our products. In sharing these additional details today, and in our approach going forward, we are determined to do right by our customers and communicate more effectively.

If you would prefer to skip ahead to review LastPass's recommended actions for protecting your account or your business, please click here for consumers or click here for business administrators.

WHAT HAPPENED AND WHAT ACTIONS DID WE TAKE?

The two incidents that we disclosed last year affected LastPass and our customers. Neither incident was caused by any LastPass product defect or unauthorized access to – or abuse of – production systems. Rather, the threat actor exploited a vulnerability in third-party software, bypassed existing controls, and eventually accessed non-production development and backup storage environments.

We have shared technical information, Indicators of Compromise (IOCs), and threat actor tactics, techniques, and procedures (TTPs) with law enforcement and our threat intelligence and forensic partners. To date, however, the identity of the threat actor and their motivation remains unknown. There has been no contact or demands made, and there has been no detected credible underground activity indicating that the threat actor is actively engaged in marketing or selling any information obtained during either incident.

Incident 1 Summary: A software engineer's corporate laptop was compromised, allowing the unauthorized threat actor to gain access to a cloud-based development environment and steal source code, technical information, and certain LastPass internal system secrets. No customer data or vault data was taken during this incident, as there is no customer or vault data in the development environment. We declared this incident closed but later learned that information stolen in the first incident was used to identify targets and initiate the second incident.

In response to the first incident, we mobilized our internal security teams, as well as resources from Mandiant. As part of the containment, eradication, and recovery process, we took the following actions:

- Removed the development environment and rebuilt a new one to ensure full containment and eradication of the threat actor.
- Deployed additional security technologies and controls to supplement existing controls.
- Rotated all relevant cleartext secrets used by our teams and any exposed certificates.

Details of the first incident and our remediation actions can be found here.

Incident 2 Summary: The threat actor targeted a senior DevOps engineer by exploiting vulnerable third-party software. The threat actor leveraged the vulnerability to deliver malware, bypass existing controls, and ultimately gain unauthorized access to cloud backups. The data accessed from those backups included system configuration data, API secrets, third-party integration secrets, and encrypted and unencrypted LastPass customer data.

In response to the second incident, we again mobilized our incident response team and Mandiant. As part of our ongoing containment, eradication, and recovery activities related to the second incident, we have taken the following actions:

- Analyzed LastPass cloud-based storage resources and applied additional policies and controls.
- Analyzed and changed existing privileged access controls.
- Rotated relevant secrets and certificates that were accessed by the threat actor.

Additional details of the attack and our remediation actions can be found here.

WHAT DATA WAS ACCESSED?

As detailed in the incident summaries, the threat actor stole both LastPass proprietary data and customer data, including the following:

Summary of data accessed in Incident 1:

- On-demand, cloud-based development and source code repositories – this included 14 of 200 software repositories.
- Internal scripts from the repositories – these contained LastPass secrets and certificates.
- Internal documentation – technical information that described how the development environment operated.

Summary of data accessed in Incident 2:

- DevOps Secrets – restricted secrets that were used to gain access to our cloud-based backup storage.

- Cloud-based backup storage – contained configuration data, API secrets, third-party integration secrets, customer metadata, and backups of all customer vault data. All sensitive customer vault data, other than URLs, file paths to installed LastPass Windows or macOS software, and certain use cases involving email addresses, were encrypted using our Zero knowledge model and can only be decrypted with a unique encryption key derived from each user's master password. As a reminder, end user master passwords are **never** known to LastPass and are not stored or maintained by LastPass – therefore, they were not included in the exfiltrated data.
- Backup of LastPass MFA/Federation Database – contained copies of LastPass Authenticator seeds, telephone numbers used for the MFA backup option (if enabled), as well as a split knowledge component (the K2 "key") used for LastPass federation (if enabled). This database was encrypted, but the separately-stored decryption key was included in the secrets stolen by the threat actor during the second incident.

Detailed information about the specific customer data impacted by these incidents can be found here.

WHAT ACTIONS SHOULD YOU TAKE TO PROTECT YOURSELF OR YOUR BUSINESS?

To better assist our customers with their own incident-response efforts, we have prepared two Security Bulletins – one for our Free, Premium, and Families consumer users, and one tailored for our Business and Teams users. Each Security Bulletin includes information designed to help our customers secure their LastPass account and respond to these security incidents in a way that we believe meets their own personal needs or their organization's security profile and environment.

- Security Bulletin**: Recommended Actions for LastPass Free, Premium, and Families** This bulletin guides our Free, Premium, and Families customers through a review of important LastPass settings designed to help secure their accounts by confirming best practices are being followed.
- Security Bulletin**: Recommended Actions for LastPass Business** This bulletin guides administrators for our Business and Teams customers through a risk assessment of LastPass account configurations and third-party integrations. It also includes information that is relevant to both non-federated and federated customers.

If you have any questions regarding the recommended actions, please contact technical support or your customer success team, both of whom are ready to help.

WHAT WE HAVE DONE TO SECURE LASTPASS

Since August, we have deployed several new security technologies across our infrastructure, data centers, and our cloud environments to further bolster our security posture. Much of this was already planned and was done in record time, as we had begun these efforts prior to the first incident.

We have also prioritized and initiated significant investments in security, privacy, and operational best practices. We have performed a comprehensive review of our security policies and incorporated changes to restrict access and privilege, where appropriate. We completed a comprehensive analysis of existing controls and configurations, and we've made the necessary changes to harden existing environments. We have also begun the work to expand the use of encryption within our application and backup infrastructure. Finally, we have begun to scope out longer-term architectural initiatives to help drive our platform evolution across LastPass.

You can click here to see a list of the work that has been completed and work that is currently on our security roadmap.

WHAT YOU CAN EXPECT FROM US GOING FORWARD

Since our December 22nd post, I have spoken to many of our business and consumer customers. I acknowledge our customers' frustration with our inability to communicate more immediately, more clearly, and more comprehensively throughout this event. I accept the criticism and take full responsibility. We have learned a great deal and are committed to communicating more effectively going forward. Today's update is a demonstration of that commitment.

Just over a year ago, GoTo and its investors announced that LastPass would become an independent company with a new leadership team. Our goal is to unlock the company's full potential and deliver on the promise of building the leading enterprise password-management platform. In late April 2022, I joined as CEO to help lead this effort.

Over the past eight months, we have hired new leaders to help drive the company's growth and execute a new strategy. Our new team includes recognized industry veterans and leaders from the security and technology industries. As part of the company's next phase of growth, we made a multi-million-dollar allocation to enhance our investment in security across people, processes, and technology. This investment drives our commitment to evolve LastPass into a leading cyber security company and ensure that we are in a position to protect ourselves and our customers against future threats.

Thank you for your understanding, guidance, and continued support.

Karim Toubba

CEO, LastPass

Karim Toubba

CEO, LastPass

More Articles

Email Address:

I'm interested in receiving blog updates about:

Cybersecurity Tips and LastPass Tricks

Product Updates

LastPass for Admins

Industry News and Updates

Submit

Topics

Uncategorized

‹ Previous

Next ›

How it Works

Go Premium

Families

Teams

Enterprise

Digital Wallet

Password Manager

Password Generator

Username Generator

LastPass Authenticator

Partners

Blog

Press

Privacy Statement

Terms of Service

Connect with us