Database Breach Incident Report

Introduction

On September 12, 2022, at 02:45 PM PT (GMT -07:00), cielo24 services lost the connection to our main database due to an attack on the database server. The system returned to full operational capacity on Tuesday, September 13, 2022, at 7:35 AM PT (GMT -07:00).

The cause of the outage appears to be a security compromise in one of our microservices, followed by an attack on our main database. The motivation for the attack seems to have been hijacking server resources for cryptocurrency mining. There is currently no evidence of disclosure of any sensitive data.

Summary of Incident Discovery and Confirmation

What data or information was involved:

- There is currently no evidence that any customer data was breached during the incident

What are we doing to ensure data security:

- The affected server environments were eradicated and rebuilt using our automated environment management
- All system credentials were immediately cycled
- All system accounts were audited
- System monitoring was expanded to improve future response time
- Additional application-layer and network-layer protections were added to the environment
- System data was quickly audited to look for unauthorized modifications; none were found

Post-Incident Activity

Following the incident, our cyber-security team is actively monitoring other resources to ensure we don't have additional follow-up breaches. We continue the investigation of our database for data damage or loss. No loss or breach of personal or other customer data is currently in evidence. The cyber security team has reinforced our database. The investigation of where the breach was initiated is still ongoing.

Timeline

- 09-12-2022, 02:45 PM PST - The cloud logs show the start of the incident
- 09-13-2022, 03:01 PM PST - DevOps team reported the system issues
- 09-12-2022, 03:03 PM PST - GCP notified cielo24 about unusual activity

- 09-12-2022, 03:10 PM PST - The DevOps team started investigating the issue
- 09-12-2022, 03:40 PM PST - System credentials were rotated and the system was partially operational
- 09-13-2022, 04:00 AM PST - Identified the exact security breach and launched remediation
- 09-13-2022, 05:45 AM PST - Initiated database restoration as a precautionary measure
- 09-13-2022, 07:40 AM PST - The system returns to fully functional operation

Breach Information

- **Total Number of Customers Where Data was Affected:** 0
- **Date(s) Breach Occurred:** 09-12-2022, 09-13-2022
- **Date(s) Breach Discovered**: 09-12-2022
- **Description of the Breach:** Microservice breach impacted the main database
- **Information disclosure:** None currently in evidence

Contact

Please be assured that cielo24 is committed to protecting customer privacy and data. We regret that this incident transpired and apologize for any inconvenience it may have caused you. If you have further questions regarding this matter, please do not hesitate to contact us. Hours of operation are Monday - Friday 8:00 AM PT - 6:00 PM PT (GMT -07:00).

Nicole Flynn
cielo24 Privacy Officer
DataSecurity@cielo24.com
805.450.4040