Zeabur 將於 2026/12/31 停止營運，部分服務 12/1 起陸續停止 閱讀公告 →

2026年10月19日

Zeabur 2026 年十月資安事件（初步報告）

攻擊者入侵了共享叢集與 GCP 專用伺服器，並讀取了存放在 Zeabur 平台資料庫中的環境變數。本文說明發生了什麼、哪些資料受影響、我們做了什麼，以及您需要做什麼。

Yuanlin Lin

本文亦提供 English、简体中文、日本語、Español和Bahasa Indonesia。

本文時間均為世界協調時間（UTC）。調查仍在進行，本文會隨進度更新。

摘要

- **發生了什麼：** 2026 年 10 月 14 日至 15 日，攻擊者使用外洩的 Zeabur 內部憑證，入侵了共享叢集、部分專用伺服器與 Zeabur 內部系統，最後讀取了平台資料庫。
- **已關閉的入口：** 攻擊者使用的叢集管理權杖、AWS 與 GCP 金鑰、內部網路節點都已撤銷或移除，管理介面與伺服器的公網 SSH 已封鎖。所有使用者都已被登出，平台存取權杖已全部撤銷。目前紀錄中，攻擊者最後的活動是 10 月 15 日 21:05。
- **影響誰：** 主要是**共享叢集上的服務**與 **GCP 專用伺服器**。存放在 Zeabur 平台資料庫中的環境變數也遭讀取；八月後已依指引把環境變數遷移到自己專用伺服器的專案，這些變數不在平台資料庫遭讀取的範圍內。

- **您需要做什麼：** 已外洩的資料仍可能被利用。請更換存放在 Zeabur 的所有密碼與金鑰，即使八月事件後已經換過。步驟見您需要做什麼。
- **根本原因：** 這起事件的根本原因在 Zeabur：長期有效的管理憑證以明文保存，並可從公網使用。詳見為什麼會發生。
- **與八月事件的關係：** 八月的輪替沒有涵蓋這次被使用的憑證；已依八月指引遷移環境變數的專案則避開了平台資料庫的外洩。詳見與八月事件的關係。

本文用語：「已確認」表示有日誌直接記錄；「研判」表示時間與內容吻合，但缺少直接紀錄；「無法確認」表示沒有紀錄可查，我們一律當作已外洩處理；「推測」表示只有間接證據支持的可能解釋，集中列在尚未證實的推測。

發生了什麼

攻擊者走了兩條路徑，最後在 Zeabur 的內部網路會合。

路徑 A：共享叢集與 AWS

1. 10 月 14 日 01:36 起，攻擊者使用 Zeabur 內部的 AWS 金鑰，01:40 起使用共享叢集的管理權杖。這些憑證以明文保存在 Zeabur 的私有設定儲存庫中。攻擊者如何取得它們，目前**無法確認**；我們推測與八月事件外洩的 GitHub App 私鑰有關，見尚未證實的推測。
2. 共享叢集的管理介面當時對公網開放，管理權杖也沒有期限。攻擊者因此能從外部存取 9 個區域的共享叢集。
3. 01:51 起，攻擊者讀取了部分系統機密。12:39 起，範圍擴大到所有服務的設定與機密，包括環境變數。有完整讀取紀錄的區域已確認讀到內容；其餘區域缺少紀錄，我們一律當作已外洩。
4. 13:40 起，攻擊者在使用者資料庫的容器內執行讀取指令。先是少數 new-api / one-api，15:41 起大量讀取 n8n，16:50 起逐表讀取部分 PostgreSQL，最後一個指令在 17:04。攻擊者共在 865 個資料庫服務執行過指令，但不是每個指令都成功。
5. 攻擊者使用叢集中另一組權限過大的金鑰，讀取了一份舊叢集的備份（**研判**）。備份中有一組可讀取 Zeabur 機密管理服務的金鑰。
6. 10 月 15 日 14:52 至 16:51，攻擊者讀取了約 53 筆正式環境機密（**已確認**）。其中包括內部網路的管理憑證、平台資料庫的帳號，以及 GitHub App 私鑰。

路徑 B：GCP 專用伺服器

1. 10 月 14 日 13:40 起，攻擊者以 root 身分登入由 Zeabur 代管於 GCP 的專用伺服器，共 101 台。
2. 這些伺服器的初始化設定以明文保存 root 密碼。攻擊者持有一把能讀取這些設定的舊 GCP 金鑰。我們**研判**攻擊者用這把金鑰取得了密碼。
3. 10 月 15 日 14:26 起，攻擊者用舊 GCP 金鑰修改伺服器設定，加入自己的 SSH 金鑰。15:05，攻擊者又從機密管理服務取得一把正式環境的 GCP 金鑰。我們在 17:17 停用舊金鑰後，攻擊者 17:28 改用這把金鑰再次加入 SSH 金鑰，我們在 17:31 也停用了它。10 月 14 日首次登入 GCP 伺服器，早於 10 月 15 日首次已知的正式環境機密讀取紀錄；不能把後者寫成前者的起點。

4. 更早之前，9 月 1 日至 5 日已有不明來源以 root 密碼登入同批伺服器，9 月 5 日當天約 98 台。是否為同一攻擊者，目前**無法確認**。

兩條路徑會合

1. 10 月 15 日 15:30，攻擊者在一台遭入侵的 GCP 伺服器上，用路徑 A 取得的內網管理憑證，讓一個節點加入 Zeabur 內部網路。
2. 內部網路的規則允許這類節點連線平台資料庫。16:10 至 16:47，攻擊者以內部唯讀帳號讀取了平台資料庫（**已確認**）。我們比對了內部網路兩端的連線紀錄與資料庫日誌。這段期間的 29 個資料庫連線都能對應到這個節點，連線中的登入與查詢也能逐一追蹤，共 8,903 筆操作紀錄。
3. 17:58，我們移除了這個節點。

事件路徑

兩條路徑在內部網路會合。箭頭旁是攻擊者在每一步利用的憑證或缺口。



一個帶有正式環境權限的節點

↓ 內網規則允許連線，再以內部唯讀帳號登入

Zeabur 平台資料庫

存放在 Zeabur 的環境變數、帳號與專案資料

圖 1：這次攻擊者在路徑 B 入侵的伺服器上，用路徑 A 取得的內網憑證加入節點。但入侵客戶伺服器並不是加入內網的必要條件。

事件期間輪替的部分憑證，後續仍遭未授權使用。 Zeabur 的叢集每日備份會保存所有機密，而攻擊者在 10 月 15 日 15:04 讀取了備份的存取金鑰。我們在 15:40 換上的新金鑰，被 16:00 的備份收錄；攻擊者在 20:30 使用了它。我們在 18:51 刪除備份的存取金鑰，並在 21:47 再次輪替受影響的憑證。新金鑰被備份收錄、之後遭使用，這兩點已確認；攻擊者是否下載了這份備份屬於研判。攻擊者可能在 18:51 前就已取得備份，所以 20:30 的使用不代表 18:51 之後仍能下載。

涉及哪些資料

系統	受影響的資料	範圍
平台資料庫	存放在 Zeabur 的服務環境變數（名稱與值）	3,218,965 筆
平台資料庫	帳號（電子郵件、使用者名稱、手機號碼等）、專案、環境與服務資料	帳號 321,810
平台資料庫	zSend API 金鑰（明文）	566 把，已撤
平台資料庫	平台存取權杖	11,536 筆，只
共享叢集	所有服務的環境變數與機密	9 個區域
共享叢集	資料庫內容	865 個資料庫
GCP 專用伺服器	伺服器上的所有資料	101 台，92 位
Hetzner、DigitalOcean 專用伺服器	伺服器的管理權限	359 台與 48 台
GitHub App	存取使用者授權的 GitHub 儲存庫	10/15 15:05 至
使用者資料庫備份	台北（tpe1）與香港（hkg1）區域的備份	兩個區域

平台資料庫。 10 月 15 日 16:10 至 16:47，攻擊者讀取了上表的資料。帳號資料包含個人頁面上的資訊，例如電子郵件、使用者名稱與手機號碼。攻擊者也搜尋了環境變數與設定檔中的 API 金鑰與私鑰。從指令內容與後續行為來看，攻擊者主要在找可以直接使用的 API 金鑰，特別是 AI 服務的金鑰：攻擊者在平台資料庫中搜尋金鑰、大量讀取 n8n 與 new-api / one-api 中的憑證，也嘗試用 Zeabur 的 AWS 金鑰呼叫 Amazon

Bedrock。這只是對攻擊者意圖的觀察；攻擊者也讀取了帳號資料，我們仍把所有讀取到的資料當作已外洩。雙重驗證與通行金鑰的資料表只被查詢了統計資訊，沒有讀取內容的紀錄。我們已撤銷所有使用者的平台存取權杖，舊權杖都無法再使用。

已遷移的環境變數不在平台資料庫遭讀取的範圍內。 八月事件後，Zeabur 提供專用伺服器的使用者輪替憑證、刪除存放在 Zeabur 的環境變數與設定檔，並一鍵遷移到自己伺服器的指引與功能。已完成遷移的專案，這些資料只存放在使用者的伺服器上，Zeabur 沒有保存，因此不在這次平台資料庫遭讀取的資料中。尚未遷移的專案，環境變數仍存放在 Zeabur，這次也遭讀取。這不排除主機入侵造成的外洩；遭入侵的 GCP 專用伺服器仍適用下方的處置建議。

冒用帳號。 攻擊者讀取了用來簽發登入憑證的金鑰，我們**研判**攻擊者用它偽造了登入憑證。攻擊者到 16:47 才大量讀取平台存取權杖，而且權杖只存雜湊值，無法解釋 16:12 就開始的冒用。10 月 15 日 16:12 至 17:19，攻擊者以兩個帳號的身分呼叫 Zeabur API，讀取帳號與專案清單；其中一個是 Zeabur 員工的帳號。這些請求沒有修改任何資源。我們在 20:25 輪替了簽章金鑰，所有使用者都已被登出。

共享叢集的資料庫。 攻擊者在 865 個資料庫的容器內執行了讀取指令。稽核紀錄只記錄指令，不記錄輸出，部分指令也因錯誤而失敗，所以每個資料庫實際被讀走多少無法確認。我們依指令內容判斷：

對象	數量	被讀取的資料
使用 PostgreSQL 的 n8n	736	第三方憑證、使用者、專案、變數與 workflow
PostgreSQL（逐表讀取）	211	每張表最多 50,000 筆；台北（tpe1）區域沒有
new-api / one-api	10	AI 服務金鑰、存取權杖與使用者
Redis	1	名稱含 token、secret 等字樣的項目
MongoDB、MariaDB	各 1	台北（tpe0）沒有指令內容，當作全部外洩

使用 PostgreSQL 的 n8n，有 602 個（檢查的 607 個中）把加密金鑰寫在環境變數中，所以 n8n 內的第三方憑證等同以明文外洩。由於此次資料讀取發生於容器內部，八月事件後的資料庫密碼輪替，並未能阻斷此次存取路徑。

另外，東京（hnd1）區域至少 2 個 PostgreSQL 自 10 月 14 日 01:51 起被植入會回連外部的程式，其中一個在 10 月 15 日 16:24 仍有回連。它的入口是否為八月外洩的密碼，目前**無法確認**。我們已在發現時通知受影響的使用者更換憑證。

GCP 專用伺服器。 調查確認，攻擊者曾以 root 權限登入 101 台伺服器，最後一次登入時間為 10 月 15 日 20:36。攻擊者另於其中 50 台伺服器新增其控制的 SSH 公開金鑰，建立持續存取途徑；並在 Zeabur 的 GCP 專案內建立 5 台虛擬機器，將 16 份客戶伺服器磁碟複本掛載至其建立的虛擬機器。

基於上述存取範圍，這 101 台伺服器均被列為可能發生資料外洩及留有未授權存取機制的受影響主機。我們已透過電子郵件通知受影響使用者，並重設相關伺服器的 root 密碼。

Hetzner 與 DigitalOcean。 管理這兩家客戶伺服器的權杖寫在內部程式碼與環境變數中，隨平台資料庫一起外洩。持有權杖可以重設密碼、重灌系統或複製磁碟。我們在 10 月 16 日 01:09 撤銷了全部權杖。兩家都沒有操作稽核紀錄；Hetzner 帳號的事件都能對應到使用者本人或系統排程，DigitalOcean 仍在比對。

Linode 與 Tencent Cloud。 Linode 890 台伺服器中，有紀錄的 847 台沒有攻擊者登入。Tencent Cloud 的管理憑證沒有遭使用的紀錄。

GitHub App。 攻擊者在 10 月 15 日 15:05 讀取了 Zeabur GitHub App 的私鑰。持有私鑰就能存取使用者授權 Zeabur 存取的儲存庫。我們在 18:54 輪替私鑰，目前沒有發現它遭使用。我們已向 GitHub Support 申請完整的稽核紀錄，尚未取得回覆。

Zeabur 內部系統。 攻擊者使用了多組 Zeabur 的 AWS 金鑰。大多數請求被拒絕，但攻擊者列出了兩個區域的使用者資料庫備份與原始碼上傳的內容；是否下載**無法確認**。攻擊者嘗試呼叫 Amazon Bedrock，全部失敗，沒有產生費用。

我們做了什麼

已完成

時間（10 月 15 日）	處置
14:43–15:56	共享叢集的管理介面只允許 Zeabur 系統連線
15:32	撤銷遭使用的叢集管理權杖；21:47 再輪替一次
17:17、17:31	停用攻擊者使用的兩把 GCP 金鑰
17:58	移除攻擊者的內網節點，並撤銷建立它的憑證
18:51	刪除叢集備份的存取金鑰
18:54	輪替 GitHub App 私鑰、付款服務金鑰與 GitHub OAuth 密鑰
18:55	移除 GCP 伺服器初始化設定中的 root 密碼
20:05–21:22	停用 24 組已外洩或無法排除外洩的 AWS 金鑰，換上權限更小的新金鑰
20:25	輪替登入簽章金鑰，所有使用者被登出
20:34–20:36	移除 GCP 伺服器預設服務帳號的權限；封鎖 GCP 伺服器的公網 SSH
20:47	撤銷全部 566 把 zSend API 金鑰

時間（10 月 15 日）	處置
21:46	Zeabur 管理的專用叢集只允許 Zeabur 系統連線
10/16 01:09	撤銷外洩的 Hetzner 與 DigitalOcean 權杖

我們也停用了寫死在程式碼中的 Tencent Cloud、阿里雲與 Linode 憑證，從 GCP 伺服器移除了攻擊者的 SSH 金鑰，並保全了各系統的稽核紀錄。

之後我們也完成了：

- 撤銷所有使用者的平台存取權杖。
- 輪替其餘遭讀取的正式環境機密，包括平台資料庫的帳號密碼，並撤銷其他外洩的憑證。
- 寄信通知 GCP 專用伺服器的使用者，並重設伺服器的 root 密碼。
- 限制只有指定的服務能連線平台資料庫。
- 叢集備份不再保存明文機密，備份金鑰與其他機密分開保存。
- 刪除攻擊者留下的磁碟複本、快照與測試資源。

進行中

- 追查設定儲存庫、舊 GCP 金鑰與 9 月初伺服器登入的外洩來源。
- 新增告警：管理權限的異常使用、在容器內執行指令、大量讀取機密或資料庫、內網加入新節點、雲端金鑰從陌生來源使用。

對服務的影響

功能	影響期間（UTC）	目前狀態
登入	10/15 20:25 起需重新登入	正常
zSend 與系統信（含登入連結）	10/15 20:00–22:02	已恢復；zSend 金鑰需重
GitHub 登入與部署	10/15 18:54–22:49	已恢復
建置	10/15 20:05–22:56；中國區至 10/16 01:44	已恢復
資料庫備份	10/15 20:33–22:13	已恢復
GCP 專用伺服器管理	10/15 17:31–20:35	已恢復；只能用網頁 SSH
專用伺服器自動續費	Tencent Cloud 10/15 22:55–10/16 01:08 失敗 154 次	已恢復；扣款已退為帳戶
Tencent Cloud 重設密碼、SSH 登入紀錄	10/15 起	已恢復
Linode 專用 Kubernetes 叢集	10/15 起	已恢復

您需要做什麼

請現在就處理，不需等待通知信。八月事件後換過的憑證，也要再換一次。

所有使用者

1. **更換環境變數中的所有憑證。** 包括 API 金鑰、雲端金鑰、資料庫密碼、簽章與加密金鑰。先到服務供應商撤銷舊的，再建立新的並重新部署。八月後已把環境變數遷移到自己專用伺服器的專案，這些變數不在這次平台資料庫讀取範圍內；若主機本身遭入侵，仍須更換主機上保存的憑證。
2. **重新登入並重新建立 Access Token。** 舊的平台存取權杖已全部撤銷。到 Access Token 管理頁面建立新的權杖，並檢查有沒有不明的請求。
3. **zSend 使用者：** 重新建立 zSend API 金鑰。
4. **GitHub 使用者：** 檢查您的 GitHub 稽核紀錄中，10 月 15 日 15:05 至 18:54 來自 Zeabur GitHub App 的操作。留意這些項目：
   - 非預期的 clone 或推送
   - 新增的 deploy key
   - 被修改的 webhook
5. **核對帳單。** 檢查各服務自 2026 年 10 月 14 日起的用量與帳單，GCP 專用伺服器使用者請回溯到 9 月 1 日。10 月 14 日是我們目前知道攻擊者最早使用憑證的時間，不代表憑證在那之前沒有外洩；如果有更早的紀錄，也請一併檢查。

共享叢集使用者

1. **在資料庫內更換密碼。** 只改 Zeabur 上的環境變數，不會改到資料庫內的密碼。換密碼也不會讓已外洩的資料失效；如果資料庫存有您使用者的密碼雜湊、登入工作階段或權杖，請一併撤銷並重新產生。
2. **n8n：** 更換 n8n 加密金鑰，並重新建立 n8n 內所有第三方憑證。
3. **new-api / one-api：** 撤銷上游 AI 服務金鑰，並重新產生存取權杖。
4. **PostgreSQL：** 檢查有沒有您不認得的角色、函式、觸發器、排程工作或擴充套件。有疑慮時，建立新資料庫並只匯入資料。
5. **台北（tpe1）與香港（hkg1）區域：** 把資料庫備份中的資料當作已外洩。

GCP 專用伺服器使用者

把伺服器當作已遭入侵：

1. **備份資料後重建伺服器。** 這是移除後門最可靠的方法。
2. **暫時無法重建時，至少：**
   - 移除 `/root/.ssh/authorized_keys` 中註解為 `@zeabur-pentest` 或您不認得的金鑰。
   - 檢查 `google-sudoers` 群組、系統帳號、crontab、systemd 服務與 k3s 工作負載。
   - 更換 root 密碼，並關閉 SSH 的密碼登入。
3. **更換伺服器上的所有憑證**，包括您自己的雲端憑證，並檢查對應帳單。
4. **對照入侵指標檢查登入紀錄**，回溯到 2026 年 9 月 1 日。

Hetzner 與 DigitalOcean 專用伺服器使用者

在控制台檢查 10 月 14 日之後 root 密碼是否被重設、系統是否被重灌，並依上方 GCP 的檢查項目確認沒有不明的登入方式。

為什麼會發生

觸發： 攻擊者持有 Zeabur 的叢集管理權杖與多組雲端金鑰。這些憑證以明文保存在設定儲存庫中。攻擊者如何取得它們，目前無法確認；最可能的路徑見尚未證實的推測。

影響範圍擴大的相關因素：

- **管理權杖生命週期與介面存取控管。** 管理權杖未設定有效期限，自 2024 年 1 月建立後未曾輪替，亦未納入八月事件後的輪替範圍；管理介面可透過公網存取。
- **機密儲存與改善進度。** 設定儲存庫、程式碼、共享叢集的服務設定及建置工作中，均存在明文儲存的金鑰。GCP 伺服器初始化設定亦保存 root 密碼，此問題已於 9 月 3 日識別，但事件發生前尚未完成修正。10 月 3 日啟動的機密遷移變更，事發時尚未合併至主要分支。
- **備份內容與金鑰隔離。** 叢集備份包含所有機密，且備份存取金鑰與其他機密存放於同一環境，形成進一步存取備份內容的途徑。事件期間輪替的部分憑證亦被後續備份收錄。
- **存取權限與資源範圍。**
  - 僅需讀取單一儲存空間的金鑰，實際具備讀取整個 AWS 帳號內儲存空間的權限。
  - GCP 伺服器的預設服務帳號具備專案層級的修改權限。
  - 內網規則允許帶有特定標籤的節點連線至平台資料庫。
  - 內部唯讀資料庫帳號具備讀取所有資料的權限。
  - 已停用服務的部署金鑰，在服務停用四個月後仍然有效。
- **內部服務與使用者服務的環境隔離。** 兩者部署於同一叢集，使攻擊者在讀取使用者設定時，亦能取得內部服務憑證。
- **偵測與稽核紀錄涵蓋範圍。** 10 月 14 日持續超過 16 小時的攻擊活動未觸發告警，團隊於翌日收到使用者回報後識別事件。由於儲存空間、GCP 與 GitHub 的存取紀錄不完整，部分存取及影響範圍目前仍無法確認。

與八月事件的關係

這是 Zeabur 不到兩個月內的第二起資安事件。許多使用者在八月後依我們的指引做了調整，也會想知道：既然做了這些措施，為什麼還會發生，兩起事件有沒有關聯。

八月後做了什麼。 我們輪替了當時確認外洩的內部金鑰，並停用 Legacy API Key。產品上，專用伺服器的專案可以把環境變數與設定檔遷移到自己的伺服器，也可以刪除 Zeabur 保存的 SSH 憑證，並查看 SSH 登入紀

錄。八月事件的通知與公告中，也建議使用者輪替憑證、刪除存放在 Zeabur 的環境變數與設定檔，並遷移到自己的伺服器。

為什麼還是發生。 八月的輪替沒有涵蓋設定儲存庫中以明文保存的叢集管理權杖與 AWS 金鑰，GCP 伺服器初始化設定中的 root 密碼也還沒修正。這次攻擊者使用的正是這些憑證。八月事件報告寫「已停用或輪替所有內部管理金鑰」，這個說法並不完整，我們在此更正。攻擊者如何取得這些憑證，目前無法確認；我們的推測見尚未證實的推測。

有做對的地方。 已依八月指引完成遷移的專案，環境變數與設定檔只存放在使用者自己的伺服器上，不在這次平台資料庫遭讀取的資料中。

時間軸

攻擊者活動與我們的應變

10 月 14 日至 15 日，各系統上的攻擊者活動與我們的處置，以 UTC 時間繪製

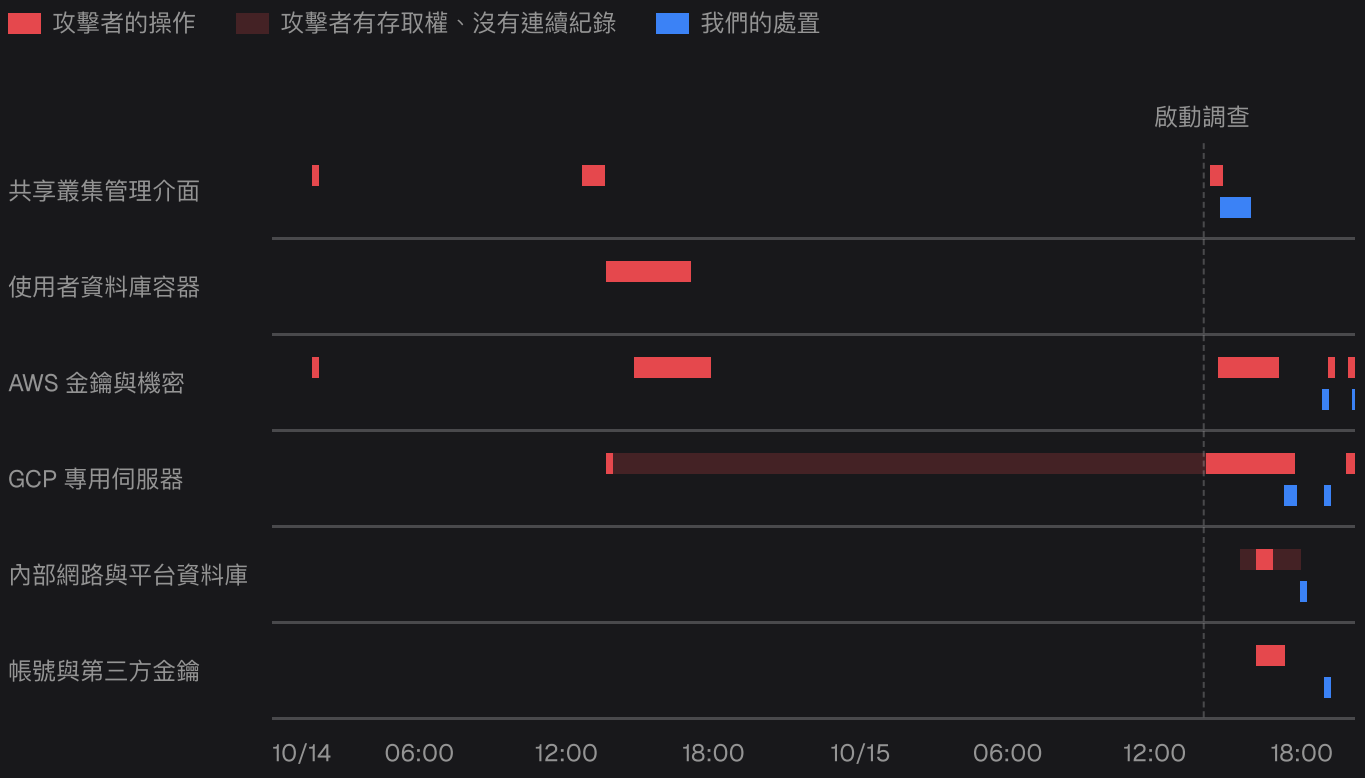


圖 2：每個系統上方是攻擊者的活動，下方是我們的處置。攻擊者使用的是有效的憑證與 Zeabur 的正式存取管道，從首次已知的憑證使用（10/14 01:36）到啟動調查約 36 小時，這段期間的存取沒有觸發告警。啟動調查後約 4 小時，已移除攻擊者的內網節點。

時間（UTC）	事件
2024 年 1 月 10 日	建立共享叢集的管理權杖，沒有期限
2026 年 1 月 20 日	管理權杖以明文寫入設定儲存庫
8 月 27 日	八月事件中，GitHub App 私鑰遭讀取；與本事件的關聯為推測
8 月 30 日、9 月 2 日	設定儲存庫以員工的 GitHub 授權被下載為壓縮檔，下載者無法確認
8 月 31 日	更換 GitHub App 私鑰；設定儲存庫中的明文憑證沒有輪替
9 月 1–5 日	不明來源以 root 密碼登入約 98 台 GCP 專用伺服器
9 月 3 日	發現 GCP 伺服器的初始化設定保存 root 密碼，未在事發前修正
10 月 10 日 18:27	後續用於憑證濫用的 IP 首次出現在 Zeabur API 存取紀錄（未登入）
10 月 13 日 21:27	攻擊者 IP 嘗試 SSH 登入 3 台專用伺服器，至 23:04，全部失敗
10 月 14 日 01:36	攻擊者首次使用 Zeabur 的 AWS 金鑰
10 月 14 日 01:40	攻擊者首次以管理權杖存取共享叢集
10 月 14 日 12:39	攻擊者讀取共享叢集所有服務的設定與機密
10 月 14 日 13:40	攻擊者開始在資料庫容器內讀取資料；同時開始登入 GCP 專用伺服器
10 月 14 日 17:04	資料庫容器內的最後一個指令
10 月 15 日 13:56	收到使用者回報後，啟動調查
10 月 15 日 14:43	開始限制共享叢集管理介面的連線來源
10 月 15 日 14:52	攻擊者開始讀取約 53 筆正式環境機密，至 16:51
10 月 15 日 15:02	已停用服務的部署金鑰讀取設定儲存庫（推測為攻擊者）
10 月 15 日 15:30	攻擊者讓一個節點加入 Zeabur 內部網路
10 月 15 日 15:42	攻擊者下載 Zeabur 儲存空間中的使用者資料庫備份
10 月 15 日 16:06	攻擊者在取得的資料中搜尋 API 金鑰，至 18:13
10 月 15 日 16:10	攻擊者開始讀取平台資料庫，至 16:47
10 月 15 日 16:12	攻擊者開始冒用帳號呼叫 API，至 17:19
10 月 15 日 17:58	移除攻擊者的內網節點
10 月 15 日 19:50	攻擊者第二波登入 GCP 專用伺服器，至 20:36
10 月 15 日 20:25	輪替登入簽章金鑰，所有使用者被登出
10 月 15 日 20:36	封鎖 GCP 專用伺服器的公網 SSH，攻擊者的登入停止
10 月 15 日 20:48	狀態頁更新為平台資料庫與專用伺服器也受影響
10 月 15 日 21:01	攻擊者嘗試存取共享叢集節點，遭拒
10 月 15 日 21:05	目前觀察到的攻擊者最後活動（AWS）

時間（UTC）	事件
10 月 16 日 01:09	撤銷 Hetzner 與 DigitalOcean 權杖
10 月 16 日 01:50	一位使用者的 OpenAI 金鑰遭濫用，至 02:56（推測來自本次外洩）

尚待釐清的事項與調查限制

以下事項因現有紀錄的涵蓋範圍或完整性限制，目前尚無法確認。對於無法排除遭未授權存取的資料與憑證，我們依可能已外洩的情境採取應變措施。

- **初始憑證的取得途徑。** 現有 GitHub 稽核紀錄未涵蓋 clone 操作，僅記錄壓縮檔下載。紀錄顯示，8 月 30 日及 9 月 2 日曾透過員工的 GitHub 授權下載設定儲存庫，但尚無法確認實際操作者。我們已請 GitHub 提供完整紀錄。目前的研判詳見尚未證實的推測。
- **共享叢集資料庫的實際資料讀取範圍。** 稽核紀錄保留了執行指令，但未記錄輸出內容，因此無法完整確認實際取得的資料。
- **備份與儲存空間物件的下載範圍。** 遭入侵主機上的證據已確認，攻擊者於 10 月 15 日 15:42 透過預先簽署的下載網址取得客戶資料庫備份。此項證據與研判涉及內部憑證外洩的叢集備份不同；後者是否遭下載，尚未確認。由於當時未啟用物件存取紀錄，其餘物件及叢集備份的實際下載範圍仍無法完整確認。
- **GCP 資源的讀取範圍。** 現有 GCP 專案紀錄未涵蓋讀取操作，目前僅能確認寫入操作。
- **Hetzner 與 DigitalOcean 權杖的使用情形。** 兩家服務未提供可供本次調查使用的操作稽核紀錄，因此無法確認相關權杖是否遭使用。
- **平台資料庫查詢回傳的具體內容。** 已確認攻擊者執行的查詢，以及其中 7 個主要查詢的回傳筆數。惟資料庫日誌未記錄回傳內容，亦無法確認攻擊者後續如何保存或使用相關資料。
- **部分叢集的活動範圍。** 台北（tpe0）叢集及攻擊者曾建立資源的專用叢集，其稽核紀錄不完整，限制了相關活動的查證範圍。
- **10 月 14 日之前的活動與影響。** 現有共享叢集及 AWS 紀錄中，未見 10 月 14 日 01:36 前使用有效憑證的活動。部分後續涉及憑證濫用的 IP，自 10 月 10 日起已出現在未登入的 Zeabur API 存取紀錄中；但這些 IP 可能由代理服務共用，無法僅憑 IP 相同確認操作者身分。10 月 13 日另有針對專用伺服器的 SSH 登入嘗試，均未成功。目前尚無法確認此期間是否發生資料外洩。

尚未證實的推測

以下是我們目前認為最可能的解釋。它們有間接證據支持，但缺少直接紀錄，不能當作事實引用。取得新證據後，我們會更新或撤回。

1. 最初的憑證可能來自八月事件

- **推測：** 攻擊者利用八月事件外洩的 GitHub App 私鑰，取得了 Zeabur 私有設定儲存庫的內容，包括 10 月 14 日使用的 AWS 金鑰與叢集管理權杖。

- **目前沒有任何證據直接證明這條路徑。** 以下只是時間與能力上吻合的間接線索。
- **哪些換了、哪些沒換：**
  - **GitHub App 私鑰：已更換。** 八月事件中，這把私鑰在 8 月 27 日遭讀取。依 GitHub 稽核紀錄與機密管理服務的版本時間，私鑰在 8 月 31 日更換，可被利用的期間約 4 天。這個 App 安裝在 Zeabur 的 GitHub 組織上，持有私鑰就能讀取組織內所有儲存庫。
  - **設定儲存庫中的明文憑證：沒有更換。** 10 月 14 日攻擊者最先使用的 AWS 金鑰與叢集管理權杖，8 月 27 日時已經以明文存在設定儲存庫中。八月事件後我們只更換了私鑰，沒有更換這些憑證，直到 10 月 15 日事件應變時才停用。因此，即使私鑰已經更換，若有人在 8 月 27 日至 31 日間取得了儲存庫內容，裡面的憑證到 10 月仍然有效。
- **其他間接線索：**
  - 攻擊者嘗試讀取的部分內部機密名稱，只出現在另一個內部儲存庫中。攻擊者可能同時持有兩個儲存庫的內容，這與 App 私鑰的組織層級權限相符。
  - 10 月 14 日 01:36 之前，共享叢集與 AWS 沒有有效憑證的使用紀錄，後來濫用憑證的 IP 在 Zeabur API 上也都沒有登入。這符合「只持有儲存庫中的憑證」的情況。
- **不支持的線索：** 八月事件與這次事件的攻擊者 IP 沒有重疊。
- **取證進度：** 我們已向 GitHub Support 申請相關紀錄，包括 8 月 27 日至 31 日間這個 App 簽發的存取權杖、設定儲存庫的 clone 與下載紀錄，以及 8 月 30 日與 9 月 2 日以員工授權下載設定儲存庫的來源。截至本文更新時尚未取得回覆。在取得紀錄前，這條路徑只是推測；員工授權的下載也不能排除是另一條取得管道。

2. 10 月 14 日前的探測可能是同一攻擊者的偵察

- **推測：** 10 月 10 日至 13 日的匿名探測與 SSH 嘗試，是同一攻擊者在使用憑證前的偵察。
- **支持的證據：**
  - `103.237.102.191`：10 月 10 日 18:27 未登入瀏覽 Zeabur，10 月 14 日以管理權杖存取共享叢集。
  - `23.106.46.239`：10 月 12 日 12:52 起未登入大量嘗試 Zeabur API，10 月 13 日嘗試 SSH 登入專用伺服器，10 月 14 日 01:36 首次使用外洩的 AWS 金鑰。
- **尚待證實：** 攻擊者大量使用代理伺服器，同一個 IP 可能由不同人共用，僅憑 IP 相同無法確認是同一人。

3. 10 月 15 日的部署金鑰存取可能是攻擊者

- **推測：** 10 月 15 日 15:02，一把已停用服務的部署金鑰讀取了設定儲存庫，研判為攻擊者所為。
- **支持的證據：** 這筆存取發生在攻擊者讀取正式環境機密期間（14:52 至 16:51）；金鑰所屬的服務已停用四個月，不應有正常存取。
- **尚待證實：** 目前沒有紀錄能把這筆存取直接連到攻擊者。

4. 外洩的使用者金鑰可能已遭濫用

- **推測：** 10 月 16 日 01:50 至 02:56，一位使用者存放在 Zeabur 的 OpenAI API 金鑰被用來發出約 1,107 次圖片生成請求。我們推測這把金鑰來自本次外洩的環境變數。
- **尚待證實：** 無法排除金鑰從其他管道外洩。這也是本文建議所有使用者更換金鑰的原因，見您需要做什麼。

入侵指標

在您的系統或服務供應商紀錄中發現下列指標時，請把相關憑證當作已外洩，並聯繫我們。攻擊者大量使用輪替的代理伺服器，下表只列代表性的位址。

類型	指標	出現在
IP	`23.106.46.239`	叢集存取、雲端
IP	`102.244.78.57`	雲端 API、GCP
IP	`103.237.102.191`	叢集存取、雲端
IP	`103.112.139.162`	首次使用叢集管
IP	`45.146.232.28`	驗證 AWS 金鑰
IP	`216.98.11.198`、`45.58.38.175`	專用伺服器 SS
IP	`52.220.72.188`	遭植入程式的 P
IP	`31.57.201.201`	9 月初以 root 登
SSH 金鑰	註解 `*@zeabur-pentest`，指紋 `SHA256:EdBc0uephoOMemIRKK0SRV2TRR45n52tJm1yErVU1iM`	攻擊者加入專用
User-Agent	`Boto3/1.43.111`（Linux 6.12.86）	攻擊者使用 AW

名詞說明

- **共享叢集（Shared Cluster）：** 多位使用者的服務一起執行的 Kubernetes 叢集。我們已在 2026 年 2 月公告退場，受影響的服務都在公告前部署。
- **專用伺服器（Dedicated Server）：** 由 Zeabur 代管、只執行單一使用者服務的伺服器。
- **管理權杖：** 能管理整個叢集的憑證，持有者可以讀取所有服務的設定並在任何容器內執行指令。
- **機密管理服務：** Zeabur 用來集中保存正式環境機密的 AWS 服務。
- **內部網路：** 連接 Zeabur 正式環境服務的私人網路（Tailscale），平台資料庫只接受這個網路的連線。
- **平台資料庫：** 保存所有帳號、專案、服務與環境變數的 Zeabur 正式資料庫。

更多資訊

如需協助，或發現異常存取與不明費用，請透過 Zeabur Support 聯繫我們。聯繫前請先撤銷相關憑證，並只提供遮蔽後的資訊；請勿在工單或公開管道貼出仍有效的金鑰或密碼。

若您的第三方 API 金鑰或雲端帳號因本事件產生額外費用，請透過支援工單申請補償。我們會核對供應商的使用紀錄與費用，並說明查核結果。

Zeabur 已宣布將於 2026 年 12 月 31 日停止營運，這是營運上的決定。在此之前，我們會持續處理本事件的支援與補償申請，並持續更新本文與狀態頁。我們向所有受影響的使用者致歉。

Zeabur 團隊

HUMAN AGENT

© 2026 Zeabur Inc.