

Google 臭蟲通報系統爆漏洞， 自家產品重大漏洞可被看光

一名研究人員在 Google 臭蟲通報系統 Google Issue Tracker 上找到三個漏洞，可以假冒的 Google.com 郵件帳號註冊、訂閱取得漏洞通知，甚至登入漏洞資料庫閱覽 Google 產品漏洞，甚至包括最嚴重等及的危險漏洞，獲得 Google 超過 1.5 萬美元的抓漏獎金。

文/[林妍濤](#) | 2017-10-31 發表

Google Issue Tracker

About Issue Tracker

Issue Tracker is a tool used internally at Google to track bugs and feature development. It is available outside of Google for use by external public and partners to collaborate with Google teams on specific projects.

Issue Tracker is not a general purpose issue-tracking tool and is not offered for external teams who want to use it for their own issue tracking. You can find a general place to submit feedback on Google products. Please refer to the individual products for instructions on providing feedback.

Google Issue Tracker 被發現存在三個漏洞，可讓駭客取得 Google 產品的重大漏洞。

Google 的內部臭蟲通報系統 Issue Tracker 被安全研究人員發現漏洞，可能導致外人得以一窺 Google 產品的漏洞資料庫，幸好在經通報後，漏洞已經由 Google 修補。

Google Issue Tracker 一般人可能不曾聽過，因為它是 Google 員工使用的產品漏洞追蹤平台，內部稱之為 Buganizer，但也提供安全研究人員向 Google 通報漏洞或特定專案合作夥伴使用。

安全研究人員 Alex Birsan 發現這個系統有三項漏洞，第一個能讓他利用 Buganizer 的帳號命名規則，成功以假冒的 Google.com 郵件帳號註冊 Buganizer，第二個使他訂閱並獲得他無權限讀取的漏洞通知。在通報 Google 後，分別獲得 3133.7 美元及 5,000 美元的抓漏獎金。

第三項漏洞則讓他透過 Buganizer API 登入 Google 後台的漏洞資料庫，可以看到數千項 Google 產品的漏洞，包括被標示為「優先程度 0」即極重大而危險的漏洞。最後一項漏洞使 Birsan 獲頒 7,500 美元的抓漏獎金。

Google 方面在發出獎金的同時，也已經修補了上述三項漏洞。

根據 [BleepingComputer](#) 報導，Alex 通報這個漏洞後一小時內就罕見地接到 Google 「抓得好！」(Nice catch!) 的回應，顯示漏洞的風險程度。一旦攻擊者只要成功入侵這項漏洞後果極嚴重，因為他可以直接使用開採漏洞，或將資料賣入黑市殃及 Google 數億用戶。微軟及 Mozilla 都曾發生過內部漏洞資料庫遭未授權存取的事。

但他也指出，駭客要從該平台上數千個漏洞中找出可用漏洞，再將之再轉化為攻擊，其實也沒那麼容易就是了。

資料來源：iThome