至少有 62 所大學網站系統遭受軟體漏洞威脅

駐芝加哥辦事處教育組

美國教育部上週三晚間發出警告，在高等教育機構中廣泛使用的一個電腦軟體存在嚴重安全性漏洞，使用者可以藉此獲得其他學生的資料及記錄。這個名為 Banner 的程式是由製造高等教育軟體的公司 Ellucian 所運營。根據 Ellucian 的網站介紹，Banner 可以用來管理學生個人資訊、財務、人力資源和獎助學金系統。美國教育部的聯邦學生援助辦公室(Federal Student Aid office)表示，已確認至少有 62 所大學因軟體漏洞遭受利用。

教育部的警告中指出，多所大學注意到有攻擊者滲透進入 Banner 系統，在「入學及註冊」的網站上建立多個假學生帳號。在過去的 24 小時裡，教育部表示「至少有 600 個假學生帳號被創建，其中一些帳號幾乎立即被用於犯罪活動」。週四，舊金山紀事報詢問哪些大學受到影響，教育部沒有回應。

任職於美國商務部底下的國家標準與技術研究所(National Institute of Standards and Technology) 的電腦科學家保羅·布萊克 (Paul E. Black) 在今年五月時曾表示，這個安全性漏洞可能會引發「非常嚴重的」問題。當時該機構評估此一漏洞的危險性為 8.1 分 (滿分 10 分)，意味著該漏洞具有嚴重的影響。布萊克表示，如果用戶成功破解了該漏洞並獲得了管理權限，他就可以更改系統中的任何資訊，包括成績和課程行事曆。更令人擔憂的是，如果大學使用 Banner 來管理他們的財務援助和線上付款系統，惡意用戶將可以竄改地址和銀行資料，把錢轉移到不同的帳戶。

布萊克說，這一漏洞是南卡羅萊納大學 (University of South Carolina) 的一名學生在 2018 年 12 月發現的。根據該學生上傳至 GitHub 的報告顯示，該學生向 Ellucian 和他的大學通報了這個問題，但直到今年 3 月底，Ellucian 才修復了這個漏洞。目前仍不清楚 Ellucian 何時或是否已經聯繫了所有使用 Banner 的大學，通知他們在發現漏洞後修補或更新他們的 Banner 系統。Ellucian 上週四向舊金山紀事報發表了一份聲明，但聲明中並未直接回答這些問題。

Ellucian 在聲明中表示，教育部指出其 8.9 版本的 Banner 最容易受到攻擊，是錯誤的資訊。該公司已將 8.9 版本修復，但較老的版本仍存在安全性漏洞。聲明中寫道：「只有 Banner Web Tailor 8.8.3 和 8.8.4 版本，以及 Banner Enterprise Identity Services (企業版) 8.3、8.3.1、8.3.2、8.4 或其他更早版本的 Banner 用戶才需要使用修復程式。」Ellucian 在其聲明中指出，駭客寫程式滲透大學資訊系統是「產業問題」，並不單只是 Ellucian 公司或 Banner 軟體的問題。大學將大量的個人資訊儲存在電子防火牆後，而試圖攻擊突破防火牆是很常見的行為。根據 Inside Higher Ed. 報導，紐約門羅大學 (Monroe College) 本月遭受駭客攻擊，關閉其網站及管理系統，並威脅該校以 200 萬美元的比特幣贖回其資訊安全。門羅大學公共事務執行長 Jackie Ruegger 稱目前該大學已經重新取得系統管理權限。

漏洞是如何運作的？

Banner 的安全性漏洞是透過「競態條件」而產生。（編按：競態條件是一種系統中不希望發生的情況，通常是指設備或系統試圖同時執行兩個或多個操作，但由於設備或系統的性質，必須按正確的順序執行操作而衍生的漏洞。）根據布萊克的解釋，競態條件可以被比喻為一個鬼鬼祟祟的小偷試圖突破建築物的門禁。假設你走到公寓大樓的保安人員面前，他需要感應你的門禁卡才能開門。當你交出門禁卡，門打開了，這時候任何潛伏徘徊在門邊的人也可以進入。這就是為什麼虛擬潛行者能夠透過複製具有管理權限用戶的電子 cookies 來進入 Banner 系統。換句話說，駭客在競態條件中率先進入了系統。

布萊克還說，一旦駭客進入 Banner 系統，除非系統保存所有的編輯紀錄，否則大學很難區辨哪些訊息被竄改了。即便系統保存了所有紀錄，也很難篩選出哪些是合法的更動，哪些不是。當然，也有一些不正當行為的跡象是比較明顯的，例如一位教授的帳號在 7 月份從另一個國家登入了網站，更改了一名學生的成績。

儘管國家標準與技術研究所將該漏洞評為 8.1 分高危險，但其使用率很低，這意味著該漏洞很難被濫用。布萊克說：「實際上，漏洞的使用難度很高，但如果駭客真的設法進入了，情況會變得很糟。」

撰稿人/譯稿人：Grace Elletson / Yung-Tsen Chen

資料來源：2019 年 7 月 18 日，The Chronicle of Higher EducationAt Least 62 Colleges Were Exploited by a Software Vulnerability. Here's What You Need to Know.