保安資訊有限公司--賽門鐵克解決方案專家--原廠防護亮點分享

Apache OFBiz 存在的多個漏洞已遭開採濫用發動攻擊，賽門鐵克用戶可高枕無憂

2024 年 10 月 23 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

Apache OFBiz 是一套開放原始碼的企業資源規劃 (ERP) 系統和商業應用程式。它提供一套企業應用軟體系統，可將企業許多業務流程整合並自動化，協助您營運整個企業。Apache OFBiz 可以多種方式用於自動化和整合業務流程，例如：供應鏈管理、庫存管理、客戶關係管理、電子商務、專案管理、人力資源等。

由於 Apache OFBiz 廣泛用於企業環境中，對於覬覦在企業環境中建立灘頭堡的攻擊者來說，它是一個具有吸引力的目標。更糟糕的是，Apache OFBiz 已被發現多個漏洞。這些漏洞主要屬於路徑／目錄遍歷漏洞和遠端程式碼執行漏洞類型。

路徑／目錄遍歷(原文Path／Directory Traversal Vulnerability也有人稱跨越／穿越)漏洞

路徑遍歷漏洞，也稱為目錄遍歷漏洞，是網頁應用程式中的安全弱點，會讓攻擊者存取網頁伺服器根目錄以外受限制檔案和目錄。我們之前已討論過這類漏洞及其影響。

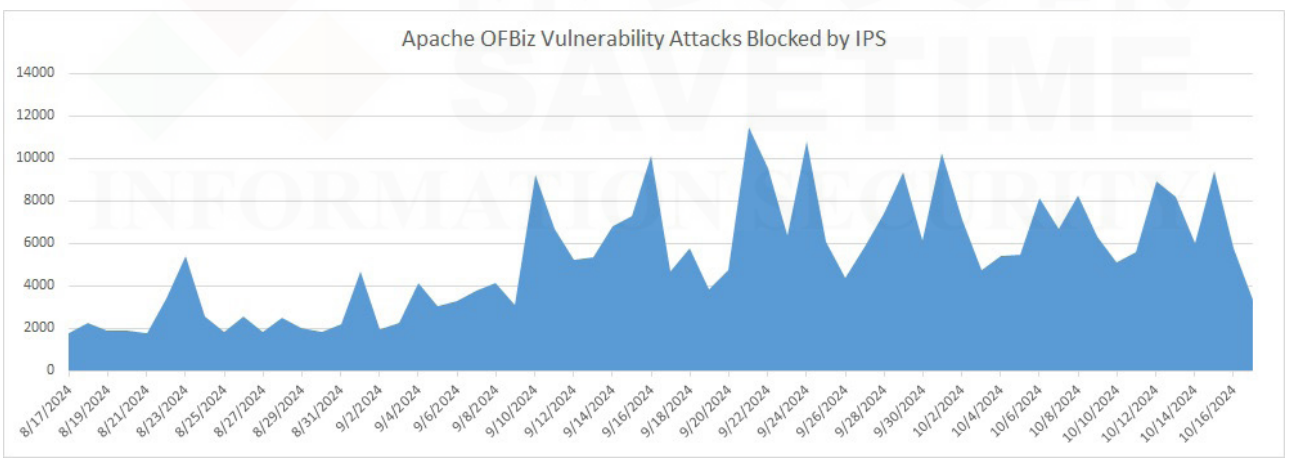
1. **CVE-2024-32113**：是存在 Apache OFBiz 的嚴重風險 (CVSS風險評分為9.1) 路徑遍歷漏洞。如果成功開採濫用此漏洞，可能會在受影響的服務帳戶導入參數執行遠端程式碼。Apache OFBiz 18.12.13 以上的版本已修補此漏洞。此漏洞也已被美國網路安全暨基礎設施安全局 (CISA)列入「已遭成功利用的高風險漏洞名單 (the Known Exploited Vulnerabilities Catalog-KEV)」中。
2. **CVE-2024-36104**：此漏洞再次被判定為嚴重風險 (CVSS風險評分為9.1) 路徑遍歷漏洞。此問題影響 18.12.14 之前的 Apache OFBiz。如果遭成功開採濫用，可讓遠端攻擊者存取未經授權的機敏檔案或目錄，並可能導致遠端執行程式碼。此漏洞是先前揭露 CVE-2024-32113 的修補程式繞過漏洞。
3. **CVE-2024-45195**：是一個高度風險 (CVSS風險評分為7.5) 的路徑遍歷漏洞，由於繞過先前 CVE-2024-32113、CVE-2024-36104 的修補程式而產生。如果遭成功開採濫用，將允許遠端攻擊者在伺服器上執行惡意程式碼，可能導致系統完全受損。此問題會影響 Apache OFBiz 18.12.16 之前的版本。

遠端程式碼執行漏洞(RCE)

遠端程式碼執行是一種允許遠端攻擊者在遠端機器上執行任意程式碼的漏洞。RCE 漏洞會危及使用者的敏感資料，讓攻擊者執行惡意程式碼或惡意軟體，並接管受影響的系統。

1. **CVE-2024-38856**：是嚴重風險等級 (CVSS風險評分為9.8) 的預先驗證 (Pre-Authentication) 遠端程式碼執行漏洞，影響 Apache OFBiz 18.12.14 之前的版本。此漏洞源自覆寫檢視功能的缺陷。一旦遭成功開採濫用，未經驗證的攻擊者可透過精心製作的請求遠端執行程式碼。應用程式供應商已釋出修補程式，在 18.12.15 或更新版本的產品中已修補此漏洞。此漏洞透過 Mirai 殭屍網路佈署。此漏洞也已被美國網路安全暨基礎設施安全局 (CISA) 列入「已遭成功利用的高風險漏洞名單 (the Known Exploited Vulnerabilities Catalog-KEV)」中。

賽門鐵克的網路防護技術入侵防護系統 (IPS) 會阻止這些漏洞利用嘗試，以防止系統受到感染/損害。攻擊會在初始階段就被攔截，而確保不會有惡意的有效負載被注入到系統上。到目前為止，IPS 已在超過 1 萬9,000 台機器上阻擋超過近 33 萬次利用這些漏洞的嘗試。



賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- Web Attack: Apache OFBiz RCE Vulnerability CVE-2024-38856
- Web Attack: Apache OFBiz Path Traversal Vulnerability CVE-2024-45195
- Web Attack: Apache OFBiz Path Traversal Vulnerability CVE-2024-36104
- Web Attack: Apache OFBiz Path Traversal Vulnerability CVE-2024-36104 2
- Web Attack: Apache OFBiz Path Traversal Vulnerability CVE-2024-32113
- Web Attack: Apache OFBiz Path Traversal Vulnerability CVE-2024-32113 2
- Web Attack: Apache OFBiz Path Traversal Vulnerability CVE-2024-32113 3

欲深入瞭解更多有關賽門鐵克端點安全完整版(SESC)的詳細資訊--Symantec Endpoint Security Complete，請點擊此處。

欲瞭解更多有關賽門鐵克端點安全入侵防護系統 (IPS) 的更多訊息，請點擊此處。

Symantec
A Division of Broadcom

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片) 軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

保安資訊
KEEPSAFE
INFORMATION SECURITY

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力專注在賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶使用情境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的求助暨諮詢對象。

保安資訊連絡電話：**0800-381-500**。