舊弱點監測平台報告及新平台注意事項

專案工作人員：周家安

電話：06-2761204

手機：0988075860

信箱：mkz855236@gmail.com

目錄

- 舊平台服務數據統計
- 舊平台困境
- 新平台使用注意事項

舊平台服務數據統計


教育部 網站應用程式弱點監測平台
成大資通安全研發中心營運點
最新消息
關於系統
下載專區
問 & 答
會員專區
帳號
密碼
登入
會員申請
目前位置：最新消息
相關連結

舊有之弱點掃描監測平台

- 成大單位自98年開始，受教育部委託，持續關注TANet連線單位之網站安全維護與防個資洩漏之工作
- 目前已累計服務50000次以上的網站弱點掃描

舊平台掃描項目

- 舊平台掃描引擎掃描項目(為OWASP 2010項目)：

1. 跨網站的入侵字串 (Cross-Site Scripting，XSS)
2. 資料隱碼注入 (SQL Injection)
3. 惡意檔案執行 (Malicious File Execution，MFE)
4. 不安全的物件參考 (Insecure Direct Object Reference，IDOR)
5. 不安全的配置管理 (Insecure Configuration Management，ICM)
6. 備份檔案 (Backup Files，BF)

舊平台服務數據統計

- 98~101年度

	統計時間	掃描網站(次數)總計
98年度	98/09~99/02	1191
99年度	99/03~99/12	2070
100年度	100/01~100/12	6258
101年度	101/01~101/12	8141

舊平台服務數據統計

- 102~105年度

	統計時間	掃描網站(次數)總計
102年度	102/01~102/12	8270
103年度	103/01~103/12	10540
104年度	104/03~104/10	6554
105年度	105/01~105/11	6310

舊平台困境

- 人員的異動
  - 舊程式碼
  - OWASP 2010

- 資料的整併
  - 佈署維運
  - 資料整合

舊平台困境

Apache Struts2的遠端執行惡意程式碼之漏洞

Apache Struts存在遠端攻擊漏洞

Apache軟體基金會(Apache Software Foundation)在9/5釋出了Struts 2.5.13，修補一個自2008年就存在的重大安全漏洞，可能允許駭客自遠端執行任意程式，呼籲用戶儘速更新。Apache Struts為一開源的網頁應用程式框架，主要用來開發Java EE網路應用程式，受到眾多企業的青睞。Igtm.com的一名安全研究人員Man Yue Mo發現該框架反序列化不可靠資料的方式出了問題，造成只要是以Struts與流行的REST通訊外掛打造的應用程式，其代管伺服器都將允許駭客自遠端執行任何程式。

Igtm主要提供自動化的程式碼分析服務，並免費供應給開源碼專案，根據Igtm的說法，此一編號為CVE-2017-9805的安全漏洞影響了2008年以來的所有Struts版本，各種採用該框架知名REST外掛程式的網路應用程式都受到波及。Mo表示，有非常多的組織使用Struts框架，且這個漏洞帶來具大的風險，因為該框架通常被用來設計公開的網路應用程式，例如航空公司的訂票系統，或者是金融機構的網路金融應用等，此外，要開採該漏洞對駭客來說極為簡單，唯一需要的工具就是瀏覽器。

根據RedMonk分析師Fintan Ryan的估計，財星（Fortune）一百大企業中，至少有65%正在使用以Struts框架建立的網路應用程式。Igtm團隊已打造了一支針對該漏洞的有效攻擊程式，只是目前並不打算公開，即使迄今尚未發現其他已知的攻擊程式，不過Igtm相信它很快就會現身。Apache軟體基金會已藉由Struts 2.5.13修補了此一漏洞，並說相關漏洞可能帶來阻斷服務或遠端程式攻擊。不論是該基金會或資安業者都呼籲Struts用戶應該立即更新。

新、舊平台交替之間

- 開發新一代平台取代
- 逐步讓舊平台停止服務
  - 依照新平台佈署情形再逐一通知
  - 減少新平台營運點數量
  - 新平台使用率

如果要停止舊平台服務

- 新平台到位

- 停止服務流程：

1. 與各位夥伴聯絡，了解使用情形
2. 遠端操作或由辦公室人員到場
3. 資料取回
4. 停止服務後將該主機資料銷毀
5. 完成停用

新平台使用注意事項


EVS
首頁
系統資訊
登入
弱點檢測平台
evs.twisc.ncku.edu.tw
© 2017 - EWSOC All rights reserved.
Secured By
TWCA
17/11/08

新平台使用注意事項提醒

- IP白名單：

由於新平台掃描時會對受測網站進行大量連線請求(Request)，資安設備可能誤判為攻擊，而將平台掃描IP封鎖。

請各位夥伴協助將以下四個檢測IP列入資安防護設備之白名單

140.116.221.36、140.116.221.37、140.116.221.38、140.116.221.39

以利日後弱點掃描作業

新平台使用注意事項提醒

- 各位夥伴拿到的網站平台帳號密碼(包含轄下單位)，需要謹慎保管，避免讓其他非相關人員得知帳號密碼，造成敏感資料外洩。
- 使用新平台同時，各位夥伴可以對教育訓練的相關課程多加了解，提升人員的資安素養

報告結束，謝謝各位聆聽