大 仁 科 技 大 學
Tajen University

管 制 文 件 訂 修 廢 履 歷 表

文件編號	資訊-程序-29	文件名稱	弱點管理程序書		
使用部門	圖書資訊館			機密等級	普通

版次	頁數	文件修訂摘要	實施日期
A.0	5	初版	99/05/24

訂修廢者	單位主管	資訊安全長

※管制文件不得擅自塗改及做記號並禁止影印。

1.目的

為使本校對主要伺服器主機、網路設備進行弱點偵測、補強作業時有一明確之規範，以降低因系統主機技術弱點而引發之攻擊的衝擊，特制定本程序書。

2.適用範圍

凡本校重要之伺服器主機、網路設備等之弱點管理，均適用本程序書。

3.參考文件

3.1 資訊-程序-23 資訊安全事件通報及危機處理管理程序書

3.2 資訊-程序-31 資訊備份管理程序書

3.3 資訊-程序-14 系統發展與維護管理程序書

3.4 資訊-程序-08 矯正及預防管理程序書。

4.名詞定義

4.1 弱點

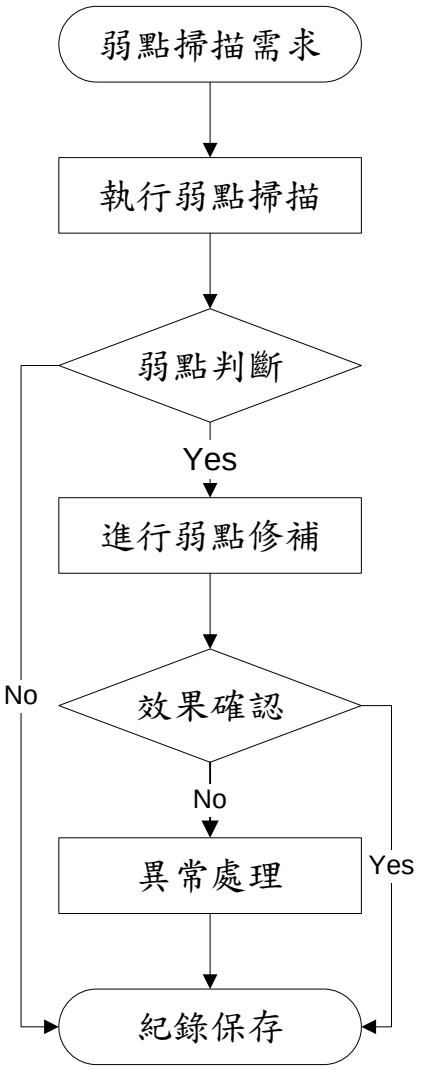
指軟硬體資訊設備上，已揭露且可被利用進行攻擊之技術漏洞。重大弱點為弱點發布單位或系統原廠所定義之嚴重、重大或應立即改善之弱點，應考量本校的防禦強度與相關安控機制，認為技術風險超出可接受範圍，應立刻著手補強。

4.2 安全性修正程式（Patch）

針對特定資訊設備技術安全性弱點所廣泛部署的修正程式，其中依據廠商定義與部署方式不同，亦可稱為更新（Update）、修補（Hotfix）或服務套件（Service Pack）等。

5.作業內容

5.1 弱點管理流程圖

流程	權責	相關文件
	圖書資訊館 圖書資訊館 圖書資訊館 圖書資訊館 圖書資訊館 圖書資訊館 圖書資訊館	資訊設備重大弱點補強紀錄表

5.2 弱點掃描需求

為確保本校各項資訊系統能持續提供穩定的服務,必須定期執行弱點掃描作業,預先找出各項資訊系統潛在的弱點,並擬定對策執行預防措施,以降低威脅及衝擊所造成的風險。

5.3 執行弱點掃描

由本校圖書資訊館或委請專業廠商,每半年定期針對電腦機房重要伺服器主機、網路設備等,進行弱點掃描,並於掃描後提出弱點掃描報告。

5.4 進行弱點判斷

5.4.1 於弱點掃描完成後,弱點掃描人員須將安全弱點列表交付各系統管理者,由各系統管理者自行或視需要取得委外服務廠商之協助,以確認弱點是否確實存在。

5.4.2 針對弱點掃描報告,圖書資訊館應親自或委由專業服務廠商,於重大弱點發現或公布時,立即進行威脅比對作業,以判別弱點與威脅是否已造成資訊安全事件,若造成資安事件則依據「資訊-程序-23 資訊安全事件通報及危機處理管理程序書」之規定辦理各項資安事件通報與處理。

5.5 進行弱點修補

對於可取得相關廠商提供安全性修補程式之弱點,得依循下列作業進行修復與測試。

5.5.變更評估作業

5.5.1.1 由圖書資訊館館長指派系統管理者依據「資訊-程序-29-01 資訊設備重大弱點補強紀錄表」,對所負責之資訊設備進行弱點補強作業。

5.5.1.2 系統管理者應於修補弱點前進行技術風險評估。須依據弱點影響性、資產重要性及弱點修復作業的可行性(例如評估部署對於網路服務效能的影響、對於停機或重新開機時間的影響等),以進行修補優先次序規劃。

5.5.1.3 系統管理者應確認安全性修補程式的來源及可靠性，避免自不明網站或郵件中下載取得。

5.5.1.4 對於重大之弱點，系統管理者須於弱點公告或弱點掃描報告提出後應儘速完成修補作業或提供其他足以降低弱點風險的控制方法。

5.5.2 安全性修補程式部署作業

5.5.2.1 弱點報告產出後，業務承辦人員須立即以系統區分將安全弱點列表並交付各系統管理者，由系統管理者對所負責之系統主機進行弱點修補作業。

5.5.2.2 系統管理者接到所負責系統主機之安全弱點列表後，須立即檢視弱點是否確實存在，並視需要取得委外服務廠商之協助進行弱點修補作業。

5.5.2.3 系統管理者需進行安全性修補程式部署前之規劃準備，包含確認部署的範圍、安全性修補程式的相依性與部署順序，及可否合併部署以減少系統重新啟動之衝擊等。

5.5.2.4 安全性修補程式部署前，亦應考慮復原程序，包括確認是否可以解除安裝部署、安排必要的程序以防電腦在部署修補程式後停止回應，以及進行適當的資料或系統備份及還原程序等。備份作業應依據「資訊-程序-31 資訊備份管理程序書」之規定辦理。

5.5.2.5 系統管理者應將安全程式部署的嚴重性、緊急性及潛在的負面影響告知單位主管。

5.5.2.6 若進行修補之標的為重要之線上系統時，於正式部署作業前，應於相似的環境進行接受度測試，以確認安全性修補程式可以在正式作業環境中正確運作。

5.5.2.7 部署時之相關變更注意事項，依據「資訊-程序-14 系統發展與維護管理程序書」之變更管理相關章節辦理。

5.5.3 部署後注意事項

於部署作業完成後，系統管理者應檢閱變更內容。包括查看相關設備之事件及系統紀錄檔，找出安全性修正程式部署之成功或失敗等相關資訊。必要時，得使用弱點掃描報告來監視更新部署狀況。

5.5.4 殘餘弱點之安全管理作業

5.5.4.1 系統弱點若因故無法成功修補，系統管理者須於「資訊-程序-29-01 資訊設備重大弱點補強紀錄表」依據修補作業實際情形說明修正作業程序、無法補強的原因、過去曾經發現但仍未補強的歷史紀錄等資訊。

5.5.4.2 對於修補作業後仍有殘餘重大弱點之重要設備，除於「資訊-程序-29-01 資訊設備重大弱點補強紀錄表」說明無法直接利用安全性修補程式之原因外，亦應說明其他因應措施以降低弱點風險。

5.6 效果確認及異常處理

弱點掃描人員每半年應利用弱點掃描報告之統計結果，分析弱點改善之狀況，並於圖書資訊館館務會議中提出檢討，弱點無法限期處理及改善，則依據「資訊-程序-08 矯正及預防管理程序書」之相關規定執行矯正與預防措施，進行問題矯正及風險預防的作業。

6.相關文件

6.1 資訊-程序-29-01 資訊設備重大弱點補強紀錄表。