

修補程式的管理

2008 年 2 月

© 香港特別行政區政府

這份文件的內容為香港特別行政區政府的財產，未經香港特別行政區政府的明文批准，不得轉載全部或部份文件內容。

免責聲明：政府盡力確保本文資料準確，但不明示或隱含保證資料準確無誤。對於因使用本文資料而引致或與之有關的任何錯誤或遺漏，香港特別行政區政府概不承擔任何法律責任。

目錄

摘要.....	2
I. 趨勢和零日攻擊 (Zero-day attack)	3
II. 修補程式管理的部署	4
做好準備	4
確認保安漏洞和獲取修補程式 (Patch)	5
評估風險和安排優先次序	6
測試修補程式	7
部署和核實修補程式	7
修補程式的分發和應用工具	7
III. 修補程式管理之管治	9
安全考慮	9
選擇修補程式管理系統解決方案的標準	10

摘要

根據美國電腦保安事故協調中心（CERT/CC）的資料，每年被發現和報導的軟件保安漏洞多達數千個¹。靈活及有效的保安修補程式管理程序已成為維護所有資訊系統安全的一個關鍵要素。由於被發現的軟件保安漏洞及需要的更新和修補越來越多，系統管理員必須有系統地控制及管理修補程式。本文提供了一些核心原則和方法，作為建立一個有效率的修補程式管理項目的參考。

¹ http://www.cert.org/stats/vulnerability_remediation.html

I. 趨勢和零日攻擊 (Zero-day attack)

根據美國電腦保安事故協調中心 (CERT/CC) 的統計數據，每年登載的軟件保安漏洞數量從 1996 年的 345 個增加到 2006 年的 8064 個²。換言之，可識別的軟件保安漏洞在過去的 10 年已經增加了 20 倍以上。

再者，攻擊者現在能夠在更短的時間內，利用新發現的保安漏洞去攻擊目標。由發現軟件保安漏洞到其相應攻擊出現的時間持續減短。此外，在軟件供應商發放相對應的修補程式前，可利用這些新保安漏洞而進行入侵的工具卻有增加的趨勢。這種情況普遍被稱為零日攻擊。

極大部份被報導的保安事故，都是由少數系統和應用程式的保安漏洞被成功入侵而造成的³。為了避免這些已知問題或保安漏洞遭到攻擊，各機構應該確保所有資訊系統管理員，已把從軟件供應商獲得的最新保安修補程式更新到系統裡，亦應定期檢查和更新修補程式、作業系統和應用程式，以保護機構內的資訊系統。修補程式的管理程序應該是及時且有效的。為了達到此目的，我們應有系統地控制及管理修補程式。

² http://www.cert.org/stats/vulnerability_remediation.html

³ <http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf>

II. 修補程式管理的部署

成功的修補程式管理需要一個強韌和有系統的程序，這個程序，也就是修補程式管理的生命週期，包含了一些關鍵的步驟：做好準備、確認保安漏洞和獲取修補程式、評估風險和安排優先次序、測試修補程式，部署和核實修補程式。

做好準備

準備的程序建議如下：

1. 編製及備存一份整個機構（pan-organisational）的硬件和軟件清單

系統管理員應該編製及備存一份清晰的硬件設備與套裝軟件的清單，並和機構內常最常用的套裝軟件的版本編號放在一起。這份清單能夠協助管理員有效地監督和確認適用於整個機構的保安漏洞和修補程式。

2. 配置標準化

應為每一個主要的資訊科技資源群組（例如用戶工作站和檔案伺服器）編製和維持標準的配置。配置標準化可簡化修補程式的測試與應用程式的更新程序，並減少修補程式管理的時間及人手。

3. 教育用戶

資訊保安是每一個人的責任，如果沒有整個機構的終端用戶之合作和參與，一個有效的修補程序是無法實行的。用戶應該瞭解到資訊科技保安和修補程式管理的重要性，而且這亦是他們每日工作的一部份。假如給終端用戶提供足夠的培訓，他們便能夠自行對工作站進行簡單的修補，這將減少系統管理員對於基本修補程式管理的工作量。對於容許遠程接達企業網絡的機構，用戶正確的保安認知尤為重要，因為用戶家中的電腦系統若有保安漏洞，將足以危及整個機構的安全。

確認保安漏洞和獲取修補程式 (Patch)

系統管理員有很多保安資料來源，幫助監控他們系統裡已安裝軟件系統的保安漏洞和修補程式。因每一類資源有其特別的領域，為了確保及時獲得最新保安修補程式的準確資料，系統管理員應參考多個發放訊息的來源。

一些普遍的資料來源有：

1. 產品供應商的網站和郵寄名單

對系統管理員來說，產品供應商的網站是最直接且可信賴的來源，使他們可獲得有關產品保安漏洞和修補程式的資訊。許多大型供應商也會維持一份支援客戶的電郵清單，用以透過電子郵件來通知客戶一些保安漏洞、修補程式和更新程式的訊息。然而，有時供應商沒有立即報導最新發現的保安漏洞，這可能因為他們不希望報導一些還未有修補程式的保安漏洞資料，因此其它保安漏洞和修補程式的資料來源是必要的。

2. 第三者保安漏洞參考網站

第三者保安漏洞參考網站是一個與產品供應商無關的網站，他們有時可能提供有關已被發現的保安漏洞更詳細的資料。這些網站涵蓋可能比產品供應商更早發布及最新發現的保安漏洞。如剛才所述，一些供應商可能選擇不發布一個還未有相關修補程式的保安漏洞。

第三者保安漏洞參考網站可以分為兩大類，電腦緊急應變小組經營的網站和保安供應商經營的網站。

- 電腦緊急應變小組經營的保安參考網站

美國電腦保安事故協調中心網站是其中一個熱門的保安漏洞參考網站，它提供新發現的保安漏洞之技術性資訊，可以支援系統管理員和保安專家評估這些保安漏洞的威脅，這些建議跟產品供應商所提供的新資訊一樣新。

- 保安供應商經營的保安參考網站/資源

有一些第三者保安漏洞參考網站提供訂閱的郵寄名單，例如 CyberTrust 所經營的 NTBugTraq⁴網站和 SecurityFocus 經營的 BugTraq⁵網站，都是很受資訊科技專家歡迎的，但是，系統管理員應該與產品供應商網站發布的資訊作出核對，以確認所有新發現保安漏洞的準確性。這些網站可能也提供新聞組功能讓系統管理員參與，使他們可以互相交流意見，但在使用和參與這些訂閱郵寄名單和新聞組時，管理員應該小心，不要涉漏敏感資料。

為了協助系統管理員可自動地接收到其負責系統的相關保安漏洞通知，一些保安漏洞警報服務便應運而生。在這類服務中，有些是免費的，但有些則需要一些訂閱的費用，如 Talisker 的網頁裡有一個保安漏洞警報服務的清單⁶，也提供 RSS 頻道讓系統管理員訂閱，從而跟進新發現的保安漏洞。

評估風險和安排優先次序

及時應變是有效修補程式管理的關鍵。在有限資源的情況下，系統管理員可能需要安排新修補程式部署的優先次序，並執行風險評估以決定應該先修補哪一個系統。一般而言，這個優先次序應該以下列的標準為基礎：

1. 保安威脅 -- 保安威脅是指任何對資訊系統的潛在危機，面對較大保安威脅的系統包括網站伺服器、電子郵件伺服器和具敏感資料的伺服器等面對高度威脅的系統。
2. 保安漏洞 -- 保安漏洞表示缺乏或僅有薄弱防衛能力而被攻擊者從中入侵。它可能是在一個伺服器上執行的有缺陷軟件服務，或是調解器未受限制的撥入接達等等。
3. 關鍵性 -- 這是一種測量系統對於商業營運的重要性或價值之評估方法。被視為關鍵任務的系統包括電子郵件伺服器、資料庫伺服器和網絡基建。

一般而言，在程式管理程序裡，面對比較大的保安威脅、或有較多的保安漏洞、或為關鍵任務的系統應有較高的優先權。

一旦一個保安漏洞已被証實，系統管理員應該確定它的風險及安排相關的行動（例如編排系統停機時間以安裝一個修補程式，再重新開機），並評估一旦獲得修補程式後，安裝一個保安修補程式的相關影響。在執行修補程式之前，系統管理員必須確定新的修補程式不會影響到整體系統和應用程式的功能。（詳情見下一段）

⁴ <http://www.ntbudtraq.com>

⁵ <http://www.securityfocus.com>

⁶ <http://www.secruitywizardry.com/alert.htm>

測試修補程式

修補程式的測試對確定新的修補程式會否影響現存軟件的正常運作是極其重要的，這項測試必須在一個與目標系統相同或非常相似的系統中進行，這保證修補程式的安裝不會對正式系統造成任何非預期的後果。

除了確定非預期的問題，修補程式的測試保證修補程式能夠跟預期一樣完整地修補保安漏洞或修正性能的問題，這個可透過下列兩點來完成：

1. 檢查檔案或配置的設定，以確定修補程式能夠按照供應商文件的描述來進行修正。
2. 用能偵測到已知保安漏洞的保安漏洞掃描器掃描主機系統。但因為保安漏洞掃描器也許不會檢查還未證實的保安漏洞，而許多保安漏洞掃描器只檢查軟件版本編號或修補程式的層級來決定保安漏洞是否存在，使這項技術不可有效地運作。

如果無法安裝修補程式，例如測試結果顯示修補程式會造成當機或嚴重干擾正常系統運作，則應該實施替代的保安控制。

部署和核實修補程式

修補系統中的保安漏洞可能只涉及修改一些配置的設定，但亦可能須要安裝軟件的新版本，並沒有單一的修補方法可適應用在所有的軟件應用系統和作業系統。產品或應用系統供應商可能提供有關如何修補保安程式和更新產品的方法，在安裝修補程式之前，系統管理員應該閱讀供應商所提供的相關文件。

此外，保安修補程式應該透過一個已制訂的更改要求程序進行，在安裝新的修補程式之前，管理員要對修補的系統進行一次完全備份，假如修補程式對系統有非預期或非計劃中的影響，就能夠快速且容易地回復系統到原先的狀態。在修補程式部署之後，系統管理員和用戶應該核實所有系統和應用程式的功能運作正常，而且他們亦應遵守擬定的保安政策和指引。

修補程式的分發和應用工具

機構可能考慮使用自動化的修補程式管理工具以加速修補程式的分發及安裝，在市場上有許多修補程式管理系統可以協助整個修補程式管理的程序自動化。在 patchmanagement.org 的網站⁷，可找到一份能提供修補程式評估及修正解決方案之修補

⁷ <http://patchmanagement.org>

程式管理系統供應商清單⁸，這網站也提供了一個之前曾在雜誌上發表的修補程式管理產品比較之網頁的連結⁹。

修補程式管理系統可以分成兩個類別：

1. 跨平台的修補程式管理系統

這個類別的產品可以處理多於一個以上的作業系統或是不同供應商的產品。

2. 特定修補程式管理解決方案的平台

這個類別的產品只支援特定的供應商或平台的修補程式，著名的例子是微軟所提供的修補程式管理工具，微軟視窗伺服器更新服務（WSUS）是一個微軟設計來協助系統管理員部署微軟產品更新和修補微軟作業系統的免費工具。

⁸ <http://patchmanagement.org/vendors.asp>

⁹ <http://patchmanagement.org/comparisons.asp>

III. 修補程式管理之管治

所有機構須要利用產品供應商推薦的最新修補程式，來修補已知的保安漏洞或風險以保護資訊系統不受破壞，或者執行其它補救性的保安措施，修補程式管理應該基於平衡保安以及因保安事故帶來的服務停頓之風險，還有因部署軟件修補程式所導致的成本、干擾和可用性的影響。

在安裝保安修補程式之前，應執行適當的風險評估和測試，以減低對資訊系統正常運作的負面影響，也應建立一個明確的操作程序，讓修補程式能夠快速地測試及部署。

風險程度因資訊系統的本質而有所不同，例如一個只在內部使用的資訊系統，比一個直接與互聯網連結、服務顧客或公眾的資訊系統，面臨較小的威脅。依照風險程度，機構應該決定每個系統適合的修補程式管理策略，包括修補程式的檢查和修補頻率，總而言之，高風險的資訊系統應該最早被處理。

當評估是否實施一個安全的修補程式時，應該評估安裝修補程式所帶來的風險。比較安裝修補程式的風險和保安漏洞所造成的影響，假如管理員決定不實施修補程式或無法獲得修補程式，應該有其它的補救措施，可能包括：

1. 關閉與保安漏洞相關的服務或功能。
2. 採用或增加接達控制。
3. 增加系統的監控以偵測和預防實際的攻擊。

安全考慮

當部署一個修補程式管理的解決方案時，應該考慮一些安全的議題：

1. 修補程式管理系統本身亦是一個應用程式，它可能有其本身的保安漏洞，應該盡快地對修補程式管理系統和其組件進行修補。
2. 應適當地保護修補程式管理的解決方案中的伺服器，因為它將成為一個中央的分配點，並對機構中所有的機器發送更新修補程式，如果修補程式管理伺服器的檔案受到病毒的感染，便會造成很大的災難。為了對抗病毒的入侵，伺服器上應安裝防毒軟件，並啟動自動安裝最新的電腦病毒識別碼和惡性程式碼之保護功能。
3. 修補程式管理系統的接達控制應該要嚴謹，在實體方面，應限制只有經過認證的人才可以接達中央的操縱台，在邏輯方面，應限制只有事先註冊的 IP 位址才能接達到中央操縱台。
4. 應該適當地保護通往修補程式管理系統的各通訊渠道，攻擊者也許能夠偷窺

到網絡通道的敏感資訊，例如授權的憑證或修補程式的狀態，從而探測哪個修補程式已被安裝在個別的系統中，並鎖定攻擊目標的保安漏洞。應用適當的保安措施（例如資料加密）去保護通過修補程式管理系統的敏感資訊¹⁰，以免敏感資料外洩。

5. 定期評估和審核修補程式管理系統的資訊科技保安風險。

選擇修補程式管理系統解決方案的標準

除了考慮特定的用戶和商業須求（如產品功能和預算的限制）外，機構在建立一個健全的修補程式管理系統解決方案時應該也考慮下列因素：

1. 保安漏洞之多寡：有些修補程式管理產品的保安漏洞比其它的產品多，機構應該選擇一個看起來較不可能成為保安漏洞的解決方案，從而減少修補其軟件的次數。應先進行一些獨立性的產品確認研究，複雜的產品表示有更多的程式碼和服務，也可能引進了更多的保安漏洞。選擇一個較簡單但發展成熟的產品可能比較明智。
2. 系統相容性：修補程式管理系統解決方案可分為以代理程式為基礎和無代理程式兩種。如果代理程式被安裝到許多電腦上時，機構應該評估對整個系統的影響（例如性能、穩定性和相容性）。
3. 供應商對新保安漏洞的回應：機構應該關注解決方案供應商對新保安漏洞之修補及更新的回應速度。
4. 簡易的部署和維護：修補程式管理的解決方案越容易部署和維護，機構所付出的成本就越低。
5. 審計追蹤：一個良好的修補程式管理解決方案應該提供廣泛的事件記錄功能，協助系統管理員更容易追蹤軟件修補和修補程式在個別系統的狀態。

¹⁰ <http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf>