Acronis

白皮書

透過 Acronis Cyber Protect 加強弱點評估和修補程式管理的重要性

輕鬆識別並解決安全漏洞

網路罪犯會使用各種方式入侵家用電腦使用者和企業。其中一種最常見且有效的手法便是入侵軟體中的弱點，而這些弱點可能存在於作業系統本身或是安裝的第三方應用程式中。如您預期的一樣，網路罪犯通常會挑選常用的應用程式和服務，讓 Windows 作業系統和熱門的第三方軟體（PDF 閱讀程式、辦公室套裝軟體、瀏覽器、封存工具等）成為常見的攻擊標的。當然，這不表示這些攻擊會放過其他的應用程式，事實上，完全不是這回事。網路罪犯會時常關注常用的軟體，以尋找具有嚴重弱點且從未加以修補的罕見應用程式。

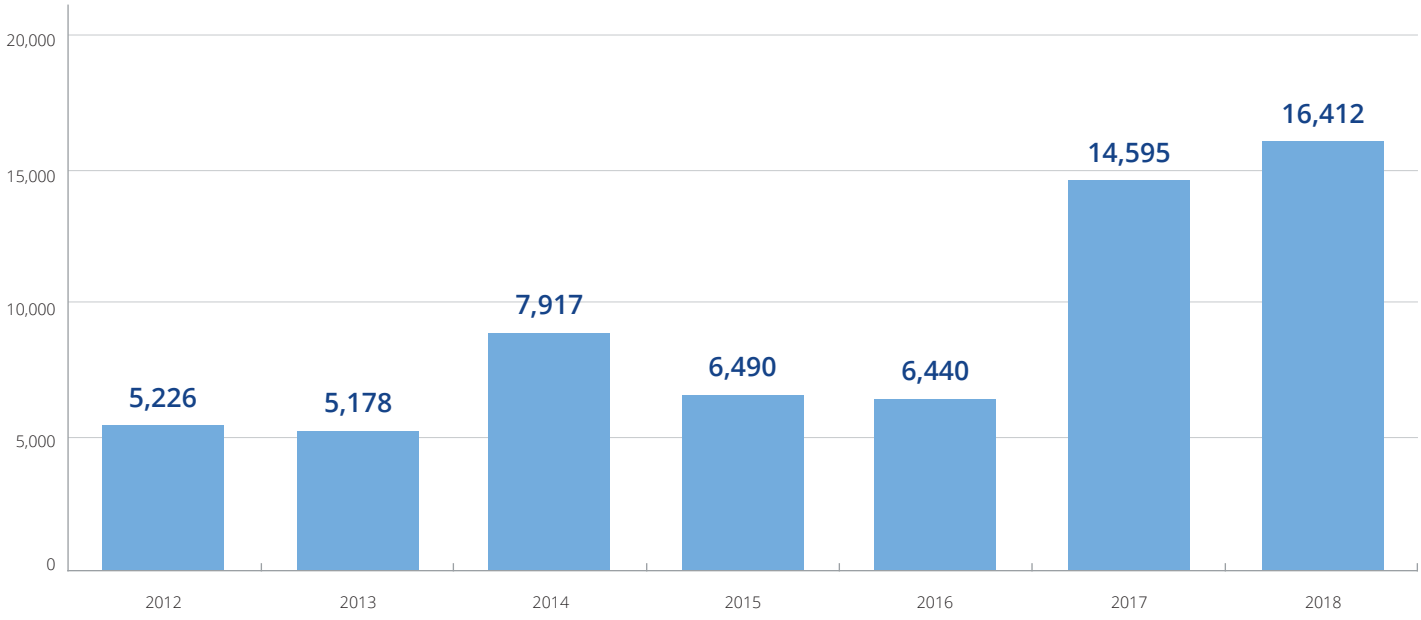
這些弱點是軟體、服務程式碼或邏輯的缺陷。所有的軟體都有弱點，畢竟是由人編寫的，讓人更在意的是，軟體內弱點的嚴重性和數量。您可以使用通用弱點評分系統（CVSS）來加以判定，這個開放式架構可以傳達軟體弱點的特性與嚴重性。CVSS 包含三個評量分組：基本、暫時和環境。基本評量的分數落在 0 到 10 之間，之後可能被時間和環境評量所修改。根據 CVSS v3.0，弱點的範圍如下：

無	低	中	高	嚴重
0.0	0.1-3.9	4.0-6.9	7.0-8.9	9.0-10.0

所有弱點都很危險，但如果軟體弱點被判定為「高」或「嚴重」，就必須立即採取行動。話雖如此，弱點要能夠被入侵（例如，在實際生活中使用）才有辦法造成損害。

弱點也不只存在於軟體上。硬體和裝置中也能發現它們的蹤影。顯然這些弱點會更難修復，近期在現代 Intel、IBM Power 和部分的 ARM 型處理器上的「熔毀」（Meltdown）和「幽靈」（Spectre）弱點便是很好的例子。這些硬體弱點會允許程式竊取目前在執行作業系統上處理的資料。

如下圖所示，弱點的數量正在持續上升。BeyondTrust 的報告指出，Microsoft 弱點在 2018 年持續增加，共找到了 700 個弱點。



Skybox Security 報告 «2019 Vulnerability and Threat Trends»

修補為何重要，又是如何運作的？

弱點可以透過軟體修補程式消除 – 這些由製造商發佈的更新檔，可用來關閉安全漏洞、新增功能或改善效能。並非所有軟體廠商都會這麼做。但不管會不會，時間落差都在所難免，因為發佈修補程式需要時間。

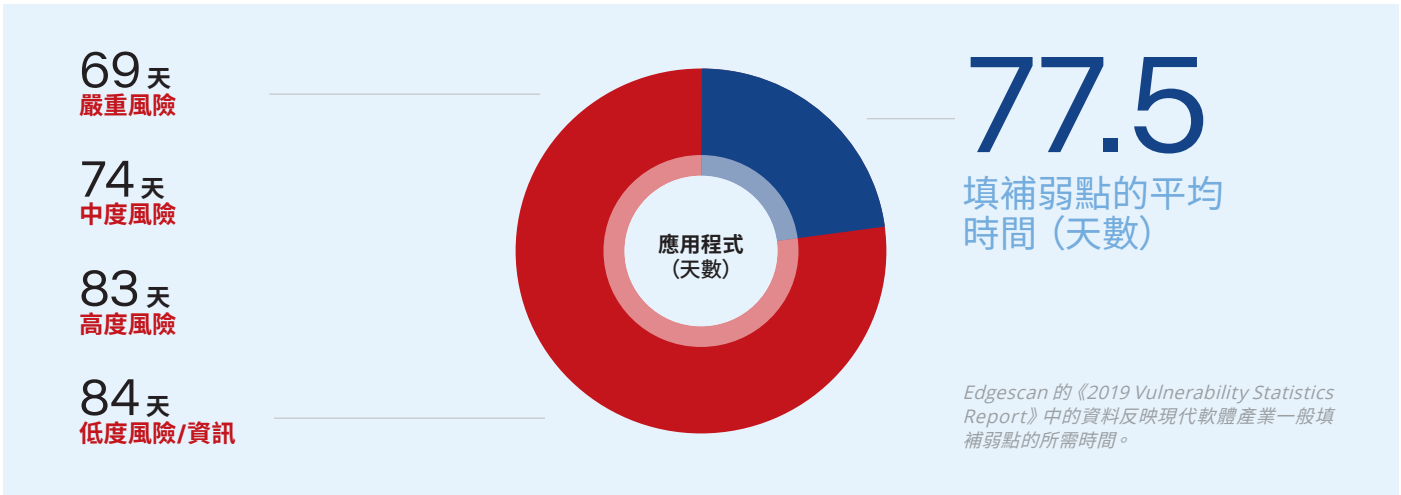
例如，目前最大的資料竊取案之一的 Equifax 資料外洩案，是透過 Apache Struts 軟體中於 2017 年 3 月 7 日揭露的已知「嚴重弱點」所執行。即使美國國土安全部已在 3 月 8 日示警，「Equifax 並未完整修補其系統 … 讓系統和資料暴露在風險中。2017 年 5 月 13 日，攻擊者對 Equifax 發動了長達 76 天的網路攻擊…」

修補通常針對支援的軟體執行。對舊版應用程式的支援一旦終止，就不該使用該應用程式，因為開發人員再也沒有義務填補安全漏洞了。

問題在於如果修補不夠透明且非自動執行，個人使用者和企業管理員就不會認真定期執行。這就是為什麼開發人員要對他們產品持續改善並自動執行更新程序。例如，Microsoft 有企業環境適用的 Windows Server Update Services (WSUS) 和家庭用戶及家庭辦公室適用的 Windows Update。Windows 應用程式有自己的更新機制。Java、Adobe、Google 和 Mozilla 等企業一般會在發佈的特定軟體中嵌入自己的更新常式。

然而，沒有一個是完美的。Microsoft 僅能更新自家軟體，卻對第三方軟體一籌莫展。其他軟體開發人員只能更新自家應用程式，並常要求使用者配合，而這也會引發問題，因為使用者為了避免作業系統重新啟動，會盡可能地拖延更新的時間。或者，使用者會安裝更新但不重新啟動機器，而機器會在重新啟動前暴露在風險中。

這就是名為修補程式管理系統的量身打造專屬的解決方案問世的原因。不幸的是，這些解決方案通常缺乏必要的功能，難以滿足客戶的期望。



一個好的修補程式管理系統能帶來什麼？

修補程式管理系統的運作方式就像個別的產品或是大型網路資安套裝軟體的一部分，旨在管理多個軟體修補程式及保持基礎架構的最新狀態，進而防護威脅入侵。在組織中，修補程式管理通常由系統管理員所控制，並會依據組織的安全原則、結構和需求（包括特定的功能需求）來進行設定。

- 不光是作業系統，也會盡可能支援應用程式。當然，您必須注意環境中使用的特定應用程式，但基本原則就是系統所涵蓋的應用程式愈多愈好。
- 自動修補程式部署可以讓系統管理員省下很多時間，在大型組織和企業中更是如此。這需和名為暫存的處理程序搭配：這個功能可以將新的修補程式安裝到特殊環境中，如果一切都執行順利的話，則會在數日後（或其他試用期間）將安裝的修補程式標示為已核准。修補程式管理的黃金法則是永遠不要對整個基礎架構部署修補程式。失敗並非不會發生，而您應該不會想讓整個組織陷入癱瘓的狀態。若要避免這點，請修補基礎架構的測試區段，並自動蒐集新修補程式可用性的資訊。
- 系統管理員必須能建立僅套用特定修補程式的自訂機器群組。這些群組通常依照部門、使用的作業系統和執行的 Java 應用程式等排列。
- 管理主控台中的修補程式狀態必須是一目瞭然，並可採取對應行動。如果修補失敗，系統管理員必須了解原因，若無法自動修復，則必須能遠端修復該狀況。管理主控台比須清楚提供所有未套用修補程式的機器，以及每個裝置的相容性狀態（例如 GDPR）。
- 因為機器離線而無法套用的修補程式應該要自動重試。通常這會發生在行動裝置和筆記型電腦上，好的修補程式管理系統會追蹤這些裝置，並在裝置上線後盡速完成修補，而不需系統管理員過度參與。
- 另外也須提供詳細的報告和通知。遺漏的修補程式、易受攻擊的系統、延遲的更新、需要重新啟動的系統，以及誰收到通知（系統管理員）等，系統管理員必須能取得這些資訊才能有效地執行工作。

> **附註：**當然這並非完整的清單，但解決這些要點才能證明企業環境中的修補程式管理系統的正當性。客戶與管理環境以邏輯方式隔離。

Acronis 弱點評估和修補程式管理

作為一家網路資安防護公司，Acronis 涵蓋了所有面向的網路資安，讓合作夥伴與客戶能順利維持永續經營。弱點評估和修補程式管理是 Acronis 網路資安防護計劃的重點項目，可以將您的安全性態勢集中在單一管理主控台和單一代理程式，藉以降低傳統安全管理的複雜性。

Acronis 弱點評估和修補程式管理功能符合上述所有的預期結果，更重要的是，全部提供在您網路上執行的裝置與應用程式的詳細資訊。弱點會依據內部嚴重性級別加以分類，且要求自動擷取更新，並微調對應的防護計劃，以各種不同的方式推送到各個群組。Acronis 會從全球佈局的雲端伺服器發送修補程式，同時也使用點對點修補程式發送技術，以避免在將修補程式推送到非 Windows 系統和第三方應用程式時發生變慢的情形。更新、升級和應用程式中可能包括內含超大檔案的套件。它們的下載與發送工作可能會消耗接收裝置的網路資源。這就是 Acronis 透過讓客戶部署中的多部裝置分攤下載這些套件的工作的最佳傳送方式，來降低頻寬使用量的原因。

與多數競爭對手的解決方案不同的是，Acronis Cyber Protect 的弱點評估不僅支援 Windows 網路，同時也支援 Linux 網路。其修補程式管理功能包含一套用戶端管理工具，可以自動化大範圍的 IT 管理功能，藉此節省時間和資源。例如，Acronis Cyber Protect 的修補程式管理功能可以修補位於公司網路內外的端點，這是擁有行動通訊用戶的客戶頻繁要求的功能。

這項修補程式管理功能可以用在從完整磁碟備份安全復原的特殊狀況中。您會意識到，您可能也備份了惡意軟體，特別是在備份整個系統時。當備份機器上沒有安裝防惡意軟體產品，或您使用的防惡意軟體解決方案不足以進行攔截時，就會發生這種情況。Acronis Cyber Protect 能夠在備份中掃描並清除惡意軟體，所以系統管理員能夠從沒有惡意軟體的「無害」磁碟映像復原使用者的機器。更重要的是，下個版本的 Acronis Cyber Protect 能自動將系統修補到最新的可用更新（如果系統管理員啟用這個選項的話），以預防全新的蠕蟲肆虐。我們的合作夥伴曾回報公司網路遭到入侵，系統管理員試圖從完整的磁碟映像復原機器時，因為網路蠕蟲惡意軟體利用了作業系統中未修補的弱點，所以又重複受到感染的實際感染案例。

將此完整磁碟備份中的 Acronis Cyber Protect 代理程式的防惡意軟體庫更新至最新的定義碼和 AI 模型，Acronis Cyber Protect 的安全復原功能就能保證您受到防護，如此您即可偵測並預防惡意軟體攻擊已完成修補的系統。

> **總結來說：**Acronis Cyber Protect 的頂級弱點評估和修補程式管理功能，因緊密整合了卓越的網路資安及獲獎肯定的備份解決方案，可提供多樣實用且獨特的功能。

修補程式管理在企業永續經營上扮演了關鍵角色

弱點評估和修補程式管理是主動式、多層次網路資安防護策略的重要部分。將新的機器註冊到網路的同時，也必須就任何已知的安全缺陷進行檢查，並在可能的情況下加以修補。如此將會提升以下各方面：

- **安全性：**資安研究人員發現弱點後，或客戶遭遇資料外洩時，通常會建立修補程式，以確保其他企業的資料、應用程式和系統將持續受到保護。重大的修補程式將盡速套用，以防止資料遭到竊取，以及因資安缺口而長期損及商譽。
- **相容性：**修補程式管理在相容性上扮演重要角色，能將潛在的資料外洩風險降到最低，並套用到資料保護上。這對因法律制裁而面臨重大損失的政府機構、醫療保健服務和金融界組織來說相當重要，而禍首正是未妥善修補弱點而導致的資料外洩。
- **生產力：**如果機器因為未經修補的弱點而遭駭且顯示為無法使用，或是在一次不理想的修補後，無法將使用者的機器復原到運作狀態，將會嚴重損及企業永續經營和生產力。好的修補程式管理解決方案可為您搞定這一切。