Microsoft 資訊安全摘要報告 3033929

推出適用於 Windows 7 和 Windows Server 2008 R2 的 SHA-2 程式碼簽署支援

發行日期：2015 年 3 月 10 日

版本： 1.0

一般資訊

提要

Microsoft 宣佈針對所有受支援版本的 Windows 7 和 Windows Server 2008 R2 重新發行更新，以增加對 SHA-2 簽署與驗證功能的支援。此更新會取代 2014 年 10 月 17 日發行的 2949927 更新，以解決部分客戶在安裝後遇到的問題。與原始版本搭配使用時，Windows 8、Windows 8.1、Windows Server 2012、Windows Server 2012 R2、Windows RT 和 Windows RT 8.1 不需要此更新，因為 SHA-2 簽署與驗證功能已包含於這些作業系統。此更新不適用於 Windows Server 2003、Windows Vista 或 Windows Server 2008。

建議。客戶若已啟用自動更新，且設定線上檢查來自於 Microsoft Update 的更新，通常無需採取任何行動，因為將會自動下載和安裝此資訊安全更新。沒有啟用自動更新的客戶則必須檢查更新，並手動安裝更新。如需有關自動更新中特定設定選項的資訊，請參閱 Microsoft 知識庫文章 294871。

本頁內容

若為手動安裝更新的客戶 (包括尚未啟用自動更新的客戶)，Microsoft 建議客戶盡早使用更新管理軟體來套用更新，或是使用 Microsoft Update 服務來檢查更新。另外亦可透過在本摘要報告中**受影響的軟體**表格所列的下載連結取得更新。

摘要報告詳細資料

問題參照

如需這個問題的詳細資訊，請參閱下列參考資料：

參考	識別
Microsoft 知識庫文件	3033929 (取代 2949927)

受影響的軟體

本次摘要報告討論下列軟體。

作業系統	取代的更新
Windows 7 32 位元系統 Service Pack 1 (3033929)[1]	MS15-025 中的 3035131
Windows 7 x64 系統 Service Pack 1 (3033929)[1]	MS15-025 中的 3035131
Windows Server 2008 R2 x64 系統 Service Pack 1 (3033929)[1]	MS15-025 中的 3035131
適用於 Itanium 型系統的 Windows Server 2008 R2 Service Pack 1 (3033929)[1]	MS15-025 中的 3035131
Server Core 安裝選項	MS15-025 中的 3035131
適用於 x64 型系統的 Windows Server 2008 R2 Service Pack 1 (Server Core 安裝) (3033929)[1]	MS15-025 中的 3035131

[1]3033929 更新與透過 MS15-025 同時發行的 3035131 更新具有共同的受影響二進位檔。手動下載並安裝更新的客戶，及計劃一併安裝兩項更新的客戶應依序安裝 3035131 和 3033929 更新。如需更多資訊，請參閱 < 摘要報告常見問題集 > 。

摘要報告常見問題集

摘要報告的範圍為何？

此摘要報告的目的是通知客戶，我們針對所有受支援版本的 Windows 7 和 Windows Server 2008 R2 提供可新增 SHA-2 雜湊演算法功能的更新。

這是需要 Microsoft 發行資訊安全更新的資訊安全風險嗎？
不是。SHA-1 的替代簽署機制已可供使用一段時間，不建議使用 SHA-1 作為簽署用途的雜湊演算法，此做法現在已並不再是最佳做法。Microsoft 建議改用 SHA-2 雜湊演算法，並發行此更新以利客戶將數位憑證金鑰移轉為更安全的 SHA-2 雜湊演算法。

SHA-1 雜湊演算法發生問題的原因為何？
問題的根本原因是 SHA-1 雜湊演算法的一項已知資訊安全風險使其可能受到碰撞攻擊。這類攻擊可允許攻擊者產生其他憑證，而該憑證具有與原始憑證相同的數位簽章。這些問題現在已釐清，因此不再鼓勵將 SHA-1 憑證用於需要對抗這些攻擊的特定用途。在 Microsoft 方面，安全性開發生命週期已要求 Microsoft 不再使用 SHA-1 雜湊演算法作為 Microsoft 軟體的預設功能。如需更多資訊，請參閱 Microsoft 資訊安全摘要報告 2880823 和 Windows PKI 部落格文章 SHA 1 取代原則。

更新的作用何在？
此更新會將 SHA-2 雜湊演算法簽署和驗證支援新增到受影響的作業系統，包括下列各項：

- 支援封包檔使用多個簽章
- 支援 Windows PE 檔案使用多個簽章
- 可供檢視多個數位簽章的 UI 變更
- 對於程式碼完整性元件上可確認核心簽章之 RFC3161 時間戳記的驗證功能
- 支援不同 API，包括 CertIsStrongHashToSign、CryptCATAdminAcquireContext2 和 CryptCATAdminCalcHashFromFileHandle2

什麼是安全雜湊演算法 (SHA-1)？
安全雜湊演算法 (SHA) 的開發目的在於配合數位簽章演算法 (DSA) 或數位簽章標準 (DSS) 使用並產生 160 位元雜湊值。SHA-1 具有已知安全風險，可能會遭受到碰撞攻擊。這類攻擊可允許攻擊者產生其他憑證，而該憑證具有與原始憑證相同的數位簽章。如需更多關於 SHA-1 的資訊，請參閱雜湊和簽章演算法。

什麼是 RFC3161？
RFC3161 會定義描述要求格式及對 Time Stamping Authority (TSA) 回應的網際網路 X.509 公開金鑰基礎結構時間戳記通訊協定 (TSP)。TSA 可用於證明數位簽章是在公開金鑰憑證的有效期間產生，請參閱 X.509 公開金鑰基礎結構。

什麼是數位憑證？
公開金鑰加密共有兩組金鑰，其中一個稱為「私密金鑰」，必須加以保密。而另一個則稱為「公開金鑰」，必須透露給外界。但是，金鑰的擁有者必須透過某種方式來告知外界金鑰的主人是誰。「數位憑證」便是金鑰擁有者用來傳達這項資訊的一種方式。一份數位憑證是一組電子認證，用來證實個人、組織、電腦的線上身分。數位憑證包含一組公開金鑰，與其相關資訊一同封包 (如金鑰的擁有者、用途、到期日等等)。詳細資訊請參閱瞭解公開金鑰加密和數位憑證。

數位憑證的用途為何？
數位憑證主要是用來確認人員或裝置的身分、驗證一項服務或加密檔案。通常，除了偶爾有指出憑證已到期或無效的訊息外，不需要思考憑證的問題。在這類情況下，應該聽從訊息中的指示。

此更新 (3033929) 如何關聯 MS15-025 中所討論的 3035131 更新？
此更新 (3033929) 與透過 MS15-025 同時發行的 3035131 更新共用受影響的二進位檔。這可避免某個更新取代其他更新的必要性，在此情況下，摘要報告更新 3033929 會取代更新 3035131。已啟用自動化更新的客戶應不會遇到不尋常的安裝行為；這兩個更新必須自動安裝，且必須出現在已安裝更新清單中。然而，若為手動下載和安裝更新的客戶，更新的安裝順序將決定觀察到的行為，如下所示：

案例 1 (慣用)：客戶第一次安裝更新 3035131，然後安裝摘要報告更新 3033929。
結果：這兩種更新應該正常安裝，且這兩種更新應該會出現在已安裝更新清單中。

案例 2：客戶先安裝摘要報告更新 3033929，然後嘗試安裝更新 3035131。
結果：安裝程式通知使用者已在系統上安裝 3035131 更新；且「未」將 3035131 的更新加入至已安裝更新清單。

建議動作

- **套用受支援 Microsoft Windows 版本的更新**
  大部分客戶都已啟用自動更新，不必採取任何行動，因為系統會自動下載和安裝此更新。沒有啟用自動更新的客戶則必須檢查更新，並手動安裝更新。如需有關自動更新中特定設定選項的資訊，請參閱 Microsoft 知識庫文章 294871。

  若是系統管理員和企業安裝，或是想要手動安裝此資訊安全更新的使用者 (包括未啟用自動更新的客戶)，Microsoft 建議客戶透過更新管理軟體或利用 Microsoft Update 服務檢查更新，以盡早套用更新。另外亦可透過在本摘要報告中**受影響的軟體**表格所列的下載連結取得更新。

其他建議動作

- **保護您的電腦**
  我們持續鼓勵客戶依照「保護您的電腦」中的指引啟用防火牆、取得軟體更新，以及安裝防毒軟體。如需更多資訊，請參閱 Microsoft 資訊安全中心。

- **維持 Microsoft 軟體的最新狀態**
  執行 Windows 軟體的使用者應套用最新的 Microsoft 資訊安全更新，以確保電腦受到盡可能完善的保護。如果您不確定軟體是否為最新，請造訪 Windows Update，掃描電腦尋找可用的更新，並安裝提供給您的任何高優先順序的更新。如果您啟用了自動更新，並將其設成為提供 Microsoft 產品更新，更新就會在發行時傳送給您，但您仍應確認更新程式已確實安裝。

其他資訊

Microsoft 主動保護計畫 (MAPP)

為了增強客戶的資訊安全保護，Microsoft 將在每月發行安全性更新之前，提前向重要資訊安全軟體提供者提供資訊安全風險資訊。資訊安全軟體提供者可利用此資訊安全風險資訊，透過其資訊安全軟體或裝置 (如防毒軟體、網路入侵偵測系統、或主機入侵預防系統)，為客戶提供更新的保護措施。如果要判斷是否有資訊安

全軟體提供者的主動保護可用，請造訪由 Microsoft 主動保護計畫 (MAPP) 合作夥伴 (英文) 上列出的計畫合作夥伴所提供的主動保護計畫網站。

意見反應

- 您可以填寫 Microsoft 技術支援服務表格 (客戶服務：與我們連絡) 來提供意見反應。

支援

- 美國及加拿大地區客戶可洽詢安全性支援以取得技術支援。如需更多資訊，請參閱 Microsoft 說明及支援。
- 不同國家的客戶，可以從當地的 Microsoft 分公司取得支援。如需更多資訊，請參閱國際支援。
- Microsoft TechNet 資訊安全網站提供 Microsoft 產品安全性的其他相關資訊。

免責聲明

本摘要報告中的資訊係以其「現狀」提供，並不提供任何形式之擔保。Microsoft 不做任何明示或默示的責任擔保，包括適售性以及適合某特定用途之擔保責任。無論任何情況下的損害，Microsoft Corporation 及其供應商皆不負任何法律責任，包括直接、間接、偶發、衍生性、所失業務利益或特殊損害。即使 Microsoft Corporation 及其供應商已被告知此類損害的可能性亦不負任何責任。某些地區不允許排除及限制衍生性或附隨損害賠償責任，因此前述限制不適用於這些地區。

修訂

- V1.0 (2015 年 3 月 10 日)：摘要報告發行。

頁面產生時間：2015-03-04 14:52Z-08:00。