106 年第四季定期弱點掃描之說明與修補方式

一、 [97742] Microsoft XML Core Services 的安全性更新 (4010321)

(一) 簡要說明

當 Microsoft XML Core Services (MSXML) 不當處理記憶體中的物件時，表示存在資訊弱點。成功利用弱點可能會讓攻擊者可以測試檔案是否存在磁碟上。 (CVE-2017-0022)

(二) 檢測方法

1. 使用弱點掃描軟體—Nessus檢測

使用Nessus掃描軟體，並且使用Plugin ID 97742進行偵測，依此判斷是否存在此弱點。

(三) 修補方式

1. 啟用微軟自動下載更新功能，保持Windows 在最新狀態。
2. 未啟用自動更新之用戶，請定期檢閱微軟釋出之安全性公告，並手動更新相關漏洞修補程式。

(四) 參考資料

https://technet.microsoft.com/zh-tw/library/security/MS17-022
http://www.tenable.com/plugins/index.php?view=single&id=97742
CVE
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0022

二、 [97735] MS17-023：Adobe Flash Player 的安全性更新 (4014329)

（一）簡要說明

在網頁式攻擊案例中，當使用者正在桌面使用 Internet Explorer，攻擊者可架設一個蓄意製作的網站，專門為透過 Internet Explorer 利用任一弱點而設計，然後引誘使用者瀏覽該網站。攻擊者也可在主控 IE 轉譯引擎的應用程式或 Microsoft Office 文件中內嵌 ActiveX 控制項，並標示為「對初始化是安全的」。攻擊者也可能利用受侵害的網站，以及接受或裝載使用者提供內容或廣告的網站。這些網站可能含有蓄意製作的內容，以利用這些弱點。不過，在任何案例中，攻擊者無法強迫使用者檢視攻擊者控制的內容。而是引誘使用者自行前往，一般的做法是設法讓使用者點選電子郵件或即時訊息中通往攻擊者網站的連結，或設法讓使用者開啟經由電子郵件傳送的附件。

(CVE-2017-2997、CVE-2017-2998、CVE-2017-2999、CVE-2017-3000、CVE-2017-3001、CVE-2017-3002、CVE-2017-3003)

（二）檢測方法

1. 使用弱點掃描軟體—Nessus檢測

使用Nessus掃描軟體，並且使用Plugin ID97735 進行偵測，依

此判斷是否存在此弱點。

（三）修補方式

1. 啟用微軟自動下載更新功能，保持Windows 在最新狀態。
2. 未啟用自動更新之用戶，請定期檢閱微軟釋出之安全性公告，並手動更新相關漏洞修補程式。
3.
4. 防止 Adobe Flash Player 執行，您可以停用 Adobe Flash Player 的初始化服務，包括在 Internet Explorer 和其他具備刪除位元功能的應用程式，例如 Office 2007 和 Office 2010，可從登錄中為控制設定刪除位元。

(四) 參考資料

https://technet.microsoft.com/zh-tw/library/security/MS17-023
http://www.tenable.com/plugins/index.php?view=single&id=97735
https://helpx.adobe.com/tw/security/products/flash-player/apsb17-07.html
CVE
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-2997
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-2998
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-2999
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-3000
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-3001
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-3002
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-3003

三、 [97744] MS17-015：Microsoft Exchange 權限提高弱點

（一）簡要說明

當 Microsoft Exchange Outlook Web Access (OWA) 無法正確處理 Web 要求時，系統中便會存在權限提高弱點。成功利用這些弱點的攻擊者可以執行指令碼或內容插入式攻擊，並嘗試誘騙使用者洩漏敏感資訊，以利用此弱點。

攻擊者可傳送內含惡意連結的蓄意製作電子郵件給使用者，以利用這些弱點。或者，攻擊者也可使用聊天用戶端，透過社交手段誘使使用者按下惡意連結。

(CVE-2017-0110)

（二）檢測方法

1. 使用弱點掃描軟體—Nessus檢測

   使用Nessus掃描軟體，並且使用Plugin ID 97744進行偵測，依此判斷是否存在此弱點。

（三）修補方式

1. 啟用微軟自動下載更新功能，保持Windows 在最新狀態。
2. 未啟用自動更新之用戶，請定期檢閱微軟釋出之安全性公告，並手動更新相關漏洞修補程式。

（四）參考資料

https://technet.microsoft.com/zh-tw/library/security/MS17-015

http://www.tenable.com/plugins/index.php?view=single&id=97744
CVE
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0110

四、 [97745] MS17-008：Windows Hyper-V 的安全性更新 (4013082)

（一）簡要說明

-多個 Hyper-V vSMB 遠端執行程式碼弱點

當主機伺服器上的 Windows Hyper-V 無法正確驗證 vSMB 封包資料時，表示存在多個遠端執行程式碼弱點。成功利用這些弱點的攻擊者可能會在目標作業系統上執行任意程式碼。

為了利用這些弱點，在虛擬機器內執行的攻擊者可能會執行蓄意製作的應用程式，造成 Hyper-V 主機作業系統執行任意程式碼。(CVE-2017-0021、CVE-2017-0095)

-多個 Hyper-V 遠端執行程式碼弱點

當主機伺服器上的 Windows Hyper-V 無法在客體作業系統上正確驗證已驗證使用者的輸入時，表示存在多個遠端執行程式碼弱點。為了利用這些弱點，攻擊者可能會在客體作業系統上執行蓄意製作的應用程式，造成 Hyper-V 主機作業系統執行任意程式碼。(CVE-2017-0075、CVE-2017-0109)

-Hyper-V 資訊洩漏弱點 – CVE-2017-0096

當主機作業系統上的 Windows Hyper-V 無法在客體作業系統上正確驗證已驗證使用者的輸入時，表示存在資訊洩漏弱點。為了利用弱點，攻擊者可能會在客體作業系統上執行蓄意製作的應用程式，造成 Hyper-V 主機作業系統洩漏記憶體資訊。成功利用弱點的攻擊者可能會取得 Hyper-V 主機作業系統資訊的存取權。(CVE-2017-0096)

（二）檢測方法

1. 使用弱點掃描軟體—Nessus檢測

使用Nessus掃描軟體，並且使用Plugin ID 97745 進行偵測，依此判斷是否存在此弱點。

（三）修補方式

1. 啟用微軟自動下載更新功能，保持Windows 在最新狀態。
2. 未啟用自動更新之用戶，請定期檢閱微軟釋出之安全性公告，並手動更新相關漏洞修補程式。

（四）參考資料

https://technet.microsoft.com/zh-tw/library/security/MS17-008
http://www.tenable.com/plugins/index.php?view=single&id=97745
CVE
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0051
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0074
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0075

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0076
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0095
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0096
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0097
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0098

五、 [96393] MS17-004：Local Security Authority Subsystem Service 的 安全性更新 (3216771)

（一）簡要說明

-Local Security Authority Subsystem Service (LSASS) 處理驗證請求的方式存在阻斷服務弱點。成功利用此弱點的攻擊者可能導致目標系統 LSASS 服務上的服務阻斷，這會觸發系統的自動重新啟動。

為了利用此弱點，未驗證的攻擊者可發送蓄意製作的驗證請求。(CVE-2017-0004)

（二）檢測方法

1. 使用弱點掃描軟體—Nessus檢測

   使用Nessus掃描軟體，並且使用Plugin ID 96393 進行偵測，依此判斷是否存在此弱點。

（三）修補方式

1. 啟用微軟自動下載更新功能，保持Windows 在最新狀態。
2. 未啟用自動更新之用戶，請定期檢閱微軟釋出之安全性公告，

並手動更新相關漏洞修補程式。

（四）參考資料

https://technet.microsoft.com/zh-tw/library/security/MS17-004
http://www.tenable.com/plugins/index.php?view=single&id=96393

CVE
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0004