106 年第三季定期弱點掃描之說明與修補方式

一、 [97833] MS17-010：Microsoft Windows SMB 伺服器的安全性更新 (4013389)

(一) 簡要說明

Microsoft Server Message Block 1.0 (SMBv1) 處理特定要求的方式中存在遠端執行程式碼弱點。成功利用弱點的攻擊者可能會獲得在目標伺服器上執行程式碼的能力。(CVE-2017-0143、CVE-2017-0144、CVE-2017-0145、CVE-2017-0146、CVE-2017-0148)

Microsoft Server Message Block 1.0 (SMBv1) 處理特定要求的方式中存在資訊洩漏弱點。成功利用此弱點的攻擊者可能會蓄意製作封包，藉此導致伺服器資訊洩漏。(CVE-2017-0147)

(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 97833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/MS17-010

http://www.tenable.com/plugins/index.php?view=single&id=97833

CVE

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0143

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0144

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0145

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0146

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0147

二、 [97743] MS17-012：Microsoft Windows 的安全性更新 (4013078)

（一）簡要說明

-當 Device Guard 無法適當地驗證已簽署 PowerShell 指令碼的特定項目時，表示存在安全性功能略過弱點。成功利用此弱點的攻擊者可能會在不讓與檔案相關之簽章失效的情況下修改 PowerShell 指令碼的內容。由於 Device Guard 依賴簽章來判斷指令碼屬於非惡意，因此 Device Guard 可能會允許惡意指令碼執行。（CVE-2017-0007）

-存在多個堆緩衝區溢出情況，將允許未經身份驗證的遠程攻擊者執行任意代碼。（CVE-2017-0016）

-當 Microsoft Windows 無法在載入某些動態連結程式庫 (DLL) 檔案之前正確地驗證輸入時，表示存在遠端執行程式碼弱點。成功利用此弱點的攻擊者可能會取得受影響系統的控制權。攻擊者接下來將能安裝程式，檢視、變更或刪除資料，或建立具有完整使用者權限的新帳戶。系統中帳戶設定為具有較少使用者權限的使用者，其所受到的影響可能會比利用系統管理使用者權限進行操作的使用者所受到的影響小。為了利用弱點，攻擊者必須先取得本機系統的存取權，並擁有執行惡意應用程式的能力。（CVE-2017-0039）

-當 Windows DNS 用戶端無法正確處理要求時，表示存在資訊洩漏弱點。成功利用此弱點的攻擊者可能會取得資訊，以便進一步侵入使用者的系統。

有多種攻擊者可以利用此弱點的方式：

如果目標是工作站，攻擊者可能會引誘使用者造訪不受信任的網頁。如果目標是伺服器，攻擊者可能必須引誘伺服器傳送 DNS 查詢到惡意 DNS 伺服器。（CVE-2017-0057）

- 若 Windows COM 工作階段 Moniker 無法在註冊 DCOM 物件時正確地強制執行 RunAs 權限，表示 Windows 存在權限提高弱點。成功利用此弱點的攻擊者可能會在其他使用者的工作階段中執行任意程式碼。攻擊者接下來將能安裝程式，檢視、變更或刪除資料，或建立具有完整使用者權限的新帳戶。

如果要利用此弱點，攻擊者首先必須登入系統。一旦其他使用者透過終端機服務或「快速切換使用者」登入相同系統，攻擊者就會執行蓄意製作的應用程式，藉此利用弱點。（CVE-2017-0100）

-當 iSNS Server 服務無法正確驗證用戶端的輸入，因而導致整數溢位時，表示 Windows 存在遠端執行程式碼弱點。成功利用此弱點的攻擊者可能會以 SYSTEM 帳戶的權限層級執行任意程式碼。

攻擊者可能會建立蓄意製作的應用程式，以連線至 iSNS Server，然後向伺服器發出惡意要求，藉此利用弱點。（CVE-2017-0104）

（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 ID97743 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/MS17-012

http://www.tenable.com/plugins/index.php?view=single&id=97743

CVE

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0007

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0016

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0039

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0057

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0100

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0104

三、 [97729] MS17-006：Internet Explorer 累積安全性更新 (4013073)

（一）簡要說明

-受影響元件處理記憶體中物件的方式中，存在資訊洩漏弱點。成功利用這些弱點的攻擊者可能會取得相關資訊來進一步侵入目標系統。

在網頁型攻擊案例中，攻擊者可能會架設網站來嘗試利用弱點。此外，受侵害的網站以及接受或存放使用者提供之內容的網站裡，也可能包含蓄意製作以利用這些弱點的內容。但是，無論如何，攻擊者無法強迫使用者檢視受攻擊者控制的內容，而是必須引誘使用者採取行動。例如，攻擊者可以引誘使用者按一下通往攻擊者網站的連結。(CVE-2017-0008、CVE-2017-0009、CVE-2017-0049、CVE-2017-0059)

-受影響的 Microsoft 瀏覽器不當存取記憶體中的物件時，即存在多個遠端執行程式碼弱點。這些弱點可能會損毀記憶體，使攻擊者有機會以目前使用者的權限層級執行任意程式碼。成功利用這些弱點的攻擊者可能會取得與目前使用者相同的使用者權限。如果目前使用者以系統管理的使用者權限登入，則攻擊者即可取得受影響系統的控制權。攻擊者接下來將能安裝程式，檢視、變更或刪除資料，或建立具有完整使用者權限的新帳戶。攻擊者可能會針對經由受影響 Microsoft 瀏覽器引起的弱點來設計並架設蓄意製作的網站，然後引誘使用者檢視該網站。攻擊者也可能利用受侵害的網站，或者接受或存放使用者提供之內容或廣告的網站 (透過新增蓄意製作以利用此弱點的內容)。

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。而是攻擊者必須引誘使用者採取動作，一般是藉助電子郵件的附件或 Instant Messenger 訊息，或是讓他們開啟經由電子郵件傳送的附件。(CVE-2017-0018、CVE-2017-0037、CVE-2017-0149)

-當 Microsoft 瀏覽器未正確剖析 HTTP 回應時，表示存在詐騙弱點。成功利用這些弱點的攻擊者可能會透過將使用者重新導向至蓄意製作的網站而誘騙使用者。蓄意製作的網站可能會偽造內容或做為樞紐，以鏈結攻擊與 Web 服務中的其他弱點。

為了利用這些弱點，使用者必須按一下蓄意製作的 URL。在電子郵件攻擊案例中，攻擊者可能會將包含蓄意製作之 URL 的電子郵件訊息傳送給使用者，以試圖說服使用者進行點選。

在網頁型攻擊案例中，攻擊者可能會架設蓄意製作的網站，且此網站的設計會讓使用者以為這是合法網站。但是，攻擊者並不能強迫使用者造訪蓄意製作的網站，攻擊者必須引誘使用者造訪蓄意製作的網站，一般是藉助電子郵件的附件或 Instant Messenger 訊息，然後引誘使用者與網站上的內容互動。(CVE-2017-0012、CVE-2017-0033)

-JScript 和 VBScript 引擎在處理 Internet Explorer 記憶體中的物件時於 Internet Explorer 呈現的方式中，存在遠端執行程式碼的多個弱點。這些弱點可能會損毀記憶體，使攻擊者有機會以目前使用者的權限層級執行任意程式碼。成功利用這些弱點的攻擊者可能會取得與目前使用者相同的使用者權限。如果

目前使用者是以系統管理使用者權限登入，成功利用這些弱點的攻擊者可能會取得受影響系統的控制權。攻擊者接下來將能安裝程式，檢視、變更或刪除資料，或建立具有完整使用者權限的新帳戶。

在網頁型攻擊的案例中，攻擊者可以針對這些經由 Internet Explorer 引起的弱點來設計並架設蓄意製作的網站，然後引誘使用者檢視該網站。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以利用此類資訊安全風險的內容。(CVE-2017-0040、CVE-2017-0130)

-當 Jscript 指令碼引擎無法正確處理記憶體中的物件時，表示存在資訊洩漏弱點。這項弱點可能會允許攻擊者偵測使用者電腦上的特定檔案。在網頁型攻擊案例中，攻擊者可能會架設網站來嘗試利用此弱點。

此外，受侵害的網站以及接受或存放使用者產生之內容的網站裡，也可能包含蓄意製作以利用本弱點的內容。但是，攻擊者無法強迫使用者檢視受攻擊者控制的內容，而是必須引誘使用者採取行動。例如，攻擊者可以引誘使用者按一下通往攻擊者網站的連結。

成功利用這個弱點的攻擊者可以讀取不應遭到洩漏的資料。請注意，此弱點不會直接允許攻擊者執行程式碼或提升使用者的權限，但能用來取得資訊，因而進一步嘗試破壞受影響的系統。

(CVE-2017-0049)

-當 Internet Explorer 未適當地強制執行跨網域原則時會存在權限提高弱點，可讓攻擊者從某個網域存取資訊並將其置於其他網域中。此更新可協助確保在 Internet Explorer 中適當地強制執行跨網域原則，進而解決這項弱點。

在網頁型攻擊案例中，攻擊者可能會架設網站來嘗試利用此弱點。此外，受侵害的網站以及接受或存放使用者提供之內容的網站裡，也可能包含蓄意製作以利用本弱點的內容。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。而是必須引誘使用者採取行動。例如，攻擊者可以引誘使用者按一下通往攻擊者網站的連結。成功利用此弱點的攻擊者可能會在受影響版本的 Internet Explorer 中提高權限。

此弱點本身不會允許執行任意程式碼。但是，此弱點可能用來搭配另一個資弱點 (例如，遠端執行程式碼的弱點)，而後者可能會利用提高的權限執行任意程式碼。例如，攻擊者可利用另一個弱點透過 Internet Explorer 執行任意程式碼，但由於程序在該內容中是由 Internet Explorer 啟動，因此會限制以較低的完整性層級 (即為有限的權限) 執行程式碼。但是，攻擊者隨後可利用此弱點而以中等完整性層級 (目前使用者的權限) 執行任意程式碼。(CVE-2017-0154)

（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 97729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/MS17-006

http://www.tenable.com/plugins/index.php?view=single&id=97729

CVE

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0008

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0009

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0012

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0018

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0033

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0037

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0040

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0049

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0059

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0130

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0149

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0154

四、 [97731] MS16-009：Microsoft Windows PDF 文件庫的安全性更新 (4010319)

（一）簡要說明

-當 Microsoft Windows PDF 文件庫不當處理記憶體中物件時，便會存在遠端執行程式碼弱點。這些弱點可能會損毀記憶體，讓攻擊者能以目前使用者的權限層級執行任意程式碼。成功利用此弱點的攻擊者可能會取得與目前使用者相同的使用者權限。如果目前使用者以系統管理的使用者權限登入，則攻擊者即可取得受影響系統的控制權。攻擊者接下來將能安裝程式，檢視、變更或刪除資料，或建立具有完整使用者權限的新帳戶。(CVE-2017-0023)

（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 97731 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/MS17-009

http://www.tenable.com/plugins/index.php?view=single&id=97731

CVE

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0023

五、 [95811] MS16-148：Microsoft Office 的安全性更新 (3204068)

（一）簡要說明

-Office 軟體無法正確處理記憶體中的物件時，Microsoft Office 軟體即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，能以目前使用者的權限層級執行任意程式碼。如果目前使用者以系統管理的使用者權限登入，則攻擊者可能會取得受影響系統的控制權。攻擊者接下來將能安裝程式，檢視、變更或刪除資料，或建立具有完整使用者權限的新帳戶。系統中帳戶設定為具有較少使用者權限的使用者，其所受到的影響可能會比利用系統管理使用者權限進行操作的使用者所受到的影響小。 (CVE-2016-7263、CVE-2016-7277、CVE-2016-7289、CVE-2016-7298)

-當 Microsoft Office 未在載入程式庫之前妥善驗證輸入時，就會存在遠端執行程式碼弱點。成功利用此弱點的攻擊者可能會取得受影響系統的控制權。攻擊者接下來將能安裝程式，檢視、變更或刪除資料，或建立具有完整使用者權限的新帳戶。系統中帳戶設定為具有較少使用者權限的使用者，其所受到的影響可能會比利用系統管理使用者權限進行操作的使用者所受到的影響小。

攻擊者必須存取本機系統，並且具備在系統上執行蓄意製作的應用程式的能力，才能利用弱點。(CVE-2016-7275)

- Office 軟體無法正確處理檔案格式剖析時，Microsoft Office 軟體會產生資訊安全功能略過弱點。略過資訊安全功能本身不

會允許執行任意程式碼。然而，若要成功利用這個弱點，攻擊者必須配合其他弱點使用，例如遠端執行程式碼弱點，才能使用資訊安全功能略過弱點，執行任意程式碼。(CVE-2016-7267)

-當 Microsoft Office 無法正確地處理輸入時，就會存在安全性功能略過弱點。成功利用此弱點的攻擊者可能會執行任意命令。

在檔案共用攻擊的案例中，攻擊者可能會提供針對弱點而設計並蓄意製作的文件檔案，然後引誘使用者開啟文件檔案，然後按一下特定儲存格與文件互動。(CVE-2016-7262)

-嘗試執行內嵌的內容時，若 Microsoft Office 無法正確地檢查登錄設定，就會存在安全性功能略過弱點。成功利用此弱點的攻擊者可能會執行任意命令。在檔案共用攻擊的案例中，攻擊者可能會提供針對弱點而設計並蓄意製作的文件檔案，然後引誘使用者多次開啟文件。(CVE-2016-7266)

-如果 Microsoft Office 無法正確處理記憶體中的物件，就會出現資訊洩漏的弱點，因而允許攻擊者擷取可能造成位址空間配置隨機載入 (ASLR) 略過的資訊。成功利用此弱點的攻擊者可能會造成資訊洩漏，以略過可保護使用者免於廣泛類別的弱點侵擾的 ASLR 安全性功能。

安全性功能略過本身不會允許執行任意程式碼。但是，攻擊者可以搭配使用 ASLR 略過弱點和其他弱點，例如搭配可利用 ASLR 略過的遠端執行程式碼弱點，即可執行任意程式碼。(CVE-2016-7257)

-當受影響的 Microsoft Office 軟體讀取作業的記憶體不足，導

致洩漏記憶體內容時，就會出現多個資訊洩漏的弱點。成功利用弱點的攻擊者可能會閱覽限制記憶。(CVE-2016-7264、CVE-2016-7265 、 CVE-2016-7268 、 CVE-2016-7276 、CVE-2016-7290、CVE-2016-7291)

- Mac 版 Microsoft AutoUpdate (MAU) 應用程式無法在執行更新前正確地進行驗證時，就會出現權限提高弱點。成功利用弱點的攻擊者已經能在系統上執行可提高權限的程式碼。為了利用弱點，攻擊者可能會在更新應用程式所使用的特定位置放置蓄意製作的可執行檔，進而以提高權限的層級執行任意程式碼。(CVE-2016-7300)

（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 95811 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/MS16-148

http://www.tenable.com/plugins/index.php?view=single&id=95811

CVE

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7263

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7264

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7265

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7266

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7267

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7268

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7275

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7276

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7277

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7289

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7290

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7291

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7298