106 年第二季定期弱點掃描之說明與修補方式

一、 [94340] MS16-128：Adobe Flash Player 的安全性更新 (3201860)

(一) 簡要說明

遠程 Windows 主機缺少 KB3201860 修補檔。因此，use-after-free error 原因將形成任意代碼執行之漏洞。未經身份驗證的遠程攻擊者，可藉由說服用戶造訪含有惡意 Flash 內容的網站，並藉由釋放的記憶體，在用戶的上下文中執行任意代碼。(CVE-2016-7855)

(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 94340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/MS16-128
http://www.tenable.com/plugins/index.php?view=single&id=94340
https://helpx.adobe.com/tw/security/products/flash-player/apsb16-3

6.html

CVE

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7855

二、 [97325] MS17-005：Adobe Flash Player 的安全性更新 (4010250)

（一）簡要說明

網站可能含有蓄意製作的內容，透過 Adobe Flash Player 的程式碼執行的記憶體損毀弱點、程式碼執行的釋放後繼續使用弱點，允許攻擊者於遠端不經授權執行程式。

Windows 主機瀏覽器上已安裝 Adobe Flash Player 擴充套件，且未更新 KB4010250 修補檔，將存在漏洞影響。

-Multiple use-after-free errors，將允許未經身份驗證的遠程攻擊者執行任意代碼。(CVE-2017-2982，CVE-2017-2985，CVE-2017-2993，CVE-2017-2994)。

-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-2017-2984，CVE-2017-2986，CVE-2017-2992)。

-存在一個整數溢出漏洞，允將允許未經身份驗證的遠程攻擊者執行任意代碼。(CVE-2017-2987)。

- 存在多個記憶體中斷問題，將允許未經身份驗證的遠程攻擊者執行任意代碼。(CVE-2017-2988，CVE-2017-2990，

CVE-2017-2991，CVE-2017-2996）。

- 存在類型混淆錯誤，將允許未經身份驗證的遠程攻擊者執行任意代碼。（CVE-2017-2995）

（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 97325 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/MS17-005
http://www.tenable.com/plugins/index.php?view=single&id=97325
https://helpx.adobe.com/tw/security/products/flash-player/apsb17-04.html
CVE
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-2982
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-2984
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-2985
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-2986
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-2987
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-2988
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-2990
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-2991
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-2992
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-2993
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-2994

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-2995
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-2996

三、 [95766] MS16-147：Microsoft Uniscribe 的安全性更新 (3204063)

（一）簡要說明

由於 Windows Uniscribe 處理記憶體中物件的方式，存在遠端執行程式碼弱點。成功利用此弱點的攻擊者可以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-2016-7274)

（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 95766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/MS16-147
http://www.tenable.com/plugins/index.php?view=single&id=95766

CVE
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7274

四、 [95764] MS16-144：Internet Explorer 累積安全性更新 (3204059)

（一）簡要說明

-多項資訊洩漏弱點

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-2016-7278、CVE-2016-7282、 CVE-2016-7284)

-多個 Microsoft 瀏覽器記憶體損毀弱點

當 Microsoft 瀏覽器不正確地存取記憶體中的物件時，即存在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。

(CVE-2016-7279、CVE-2016-7283)

- Microsoft 瀏覽器安全性功能略過弱點

當 Microsoft 瀏覽器無法針對 Web 工作者內執行的指令碼正確地套用相同來源原則時，即存在安全性功能略過弱點。

攻擊者可能誘騙使用者載入含有惡意內容的頁面。為了利用此弱點，攻擊者需要誘騙使用者載入頁面或造訪網站。此頁面也可能植入被駭網站或廣告網路中。CVE-2016-7281)

-多個指令碼引擎記憶體損毀弱點

Microsoft 指令碼引擎在處理 Microsoft 瀏覽器記憶體中的物件時，其呈現的方式中存在多個遠端執行程式碼的弱點。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。如果目前的使用者以系統管理使用者權限登入，則成功利用這些弱點的攻擊者可以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-2016-7202、CVE-2016-7287)

（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 ID95764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/MS16-144
http://www.tenable.com/plugins/index.php?view=single&id=95764

CVE
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7202
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7278
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7279
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7281
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7282
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7283
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7284
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7287

五、 [94631] MS17-001：Microsoft Edge 的安全性更新 (3214288)

（一）簡要說明

- Microsoft Edge 權限提高弱點

當 Microsoft Edge 未使用空白頁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。成功利用此弱點的攻擊者可以在受影響版本的 Microsoft Edge 中提高權限。 (CVE-2017-0002)

（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 94631 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/MS17-001
http://www.tenable.com/plugins/index.php?view=single&id=96390

CVE
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0002