106 年第一季偵測弱點掃描之說明與修補方式

一、 [94633] MS16-132Microsoft 圖形元件的安全性更新 (3199120)

(一) 簡要說明

Windows 字型資源庫不當處理蓄意製作的內嵌字型時，即會存在弱點。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-2016-7256)

當 ATMFD 元件不當洩漏其記憶體中的內容時，就會存在資訊洩漏弱點。成功利用此弱點的攻擊者可取得相關資訊來進一步侵入使用者的系統。(CVE-2016-7210)

Windows 動畫管理員不當處理記憶體中物件時，便會存在遠端執行程式碼弱點。成功利用這項弱點的攻擊者可以安裝程式，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-2016-7205)

當 Windows 媒體基礎不當處理記憶體中物件時，便會存在記憶體損毀弱點。成功利用這項弱點的攻擊者可以安裝程式，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-2016-7217)

(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 94633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/MS16-132
http://www.nessus.org/plugins/index.php?view=single&id=94633
CVE
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7205
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7210
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7217
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7256

二、 [94642]MS16-141：Adobe Flash Player 的安全性更新 (3202790)

（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。

(CVE-2016-7857、CVE-2016-7858、CVE-2016-7859、CVE-2016-7860、CVE-2016-7861、CVE-2016-7862、CVE-2016-7863、CVE-2016-7864、CVE-2016-7865)

（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 94642 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/MS16-141
http://www.nessus.org/plugins/index.php?view=single&id=94642

CVE
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7857

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7858
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7859
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7860
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7861
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7862
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7863
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7864
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7865

三、 [94643] MS16-142：Internet Explorer 累積安全性更新 (3198467)

（一）簡要說明

Microsoft 瀏覽器處理記憶體中物件的方式中，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，讓攻擊者能以目前使用者的權限層級執行任意程式碼。成功利用這些弱點的攻擊者可以取得與本機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-2016-7195 、 CVE-2016-7196 、 CVE-2016-7198 、 CVE-2016-7241)

當受影響的 Microsoft 瀏覽器不當允許跨框架互動時，即存在資訊洩漏的弱點。成功利用此弱點的攻擊者，可能會從其他網域取得瀏覽器框架或視窗狀態。

為了成功展開攻擊，攻擊者必須引誘使用者從安全網站中開啟惡意網站。這個更新會拒絕物件模型狀態的讀取權限，使不同網域中的框架或視窗無法存取，藉此解決弱點。(CVE-2016-7199)

當受影響的 Microsoft 指令碼引擎不當處理記憶體中物件時，就會存在資訊洩漏的弱點。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。(CVE-2016-7227)

Microsoft 瀏覽器 XSS 篩選在遭受漏出敏感頁面資訊攻擊時，便存在資訊洩漏弱點。成功利用這項弱點的攻擊者可以從特定化網頁獲取敏感資訊。(CVE-2016-7239)

（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 94643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/MS16-142
http://www.nessus.org/plugins/index.php?view=single&id=94643
CVE
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7195
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7196
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7197
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7198
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7199
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7227
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7239
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7241

四、 [94630]MS16-129：Microsoft Edge 的累積安全性更新 (3199057)

（一）簡要說明

Microsoft 瀏覽器處理記憶體中物件的方式中，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，讓攻擊者能以目前使用者的權限層級執行任意程式碼。(CVE-2016-7195、CVE-2016-7196、CVE-2016-7198、CVE-2016-7241)

當 Microsoft 瀏覽器不當處理記憶體中物件時，就會存在資訊洩漏的弱點。成功利用這項弱點的攻擊者，可允許攻擊者從另一端獲取瀏覽器視窗的情況。(CVE-2016-7199)

Microsoft 瀏覽器 XSS 篩選在遭受漏出敏感頁面資訊攻擊時，便存在資訊洩漏弱點。成功利用這項弱點的攻擊者可以從特定化網頁獲取敏感資訊。(CVE-2016-7239)

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遠端執行程式碼的弱點。此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。成功利用此弱點的攻擊者可以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-2016-7200、CVE-2016-7201、CVE-2016-7202、CVE-2016-7203、CVE-2016-7208、CVE-2016-7240、CVE-2016-7242、CVE-2016-7243)

當 Microsoft Edge 不當處理記憶體中物件時，就會存在資訊洩漏的弱點。成功利用此弱點的攻擊者可以追蹤使用者進入允許存取使用者的我的檔案。(CVE-2016-7204)

Microsoft Edge 未妥善剖析 HTTP 內容時存在詐騙弱點。成功利用此弱點的攻擊者可透過將使用者重新導向至蓄意製作的網站而誘騙使用者。蓄意製作的網站可偽造內容，或作為樞紐以鏈結攻擊與 Web 服務中的其他弱點。(CVE-2016-7209)

當 Internet Explorer , Edge 或 Scripting Engine 不當處理記憶體中物件時，就會存在資訊洩漏的弱點。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。(CVE-2016-7227)

（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 ID94630 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/MS16-129
http://www.nessus.org/plugins/index.php?view=single&id=94630
CVE
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7195
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7196
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7198
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7199
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7200
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7201
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7202
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7203
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7204
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7208
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7209
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7227
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7239
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7240
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7241
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7242
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7243

五、 [94631]MS16-130：Microsoft Windows 的安全性更新 (3199172)

（一）簡要說明

當 Windows 輸入法編輯器不恰當的處理 DLL 的載入時，存在權限提高弱點。為了利用此弱點，在本機驗證的攻擊者可能會執行蓄意製作的應用程式。(CVE-2016-7221)

當使用者建立使用 UNC 路徑的工作時，工作排程器即存在權限提高弱點。成功利用此弱點的攻擊者能執行任意程式碼，取得提高的系統權限。若要成功利用弱點，本機驗證的攻擊者可能會使用 Windows 工作排程器，排程使用蓄意製作之 UNC 路徑的新工作。(CVE-2016-7222)

當 Windows 的圖片檔案載入功能沒有適當處理錯誤的圖片檔案，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執行任意程式碼。(CVE-2016-7212)

（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/MS16-130
http://www.nessus.org/plugins/index.php?view=single&id=94631

CVE
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7212
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7221
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7222