105 年第四季偵測弱點掃描之說明與修補方式

一、 [92824]Microsoft Windows PDF 文件庫的安全性更新 (3182248)

(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管理使用者權限登入，攻擊者可控制受到影響的系統。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。

若將 Microsoft Edge 設為預設瀏覽器，攻擊者可利用 Windows 10 系統的弱點，架設含有惡意 PDF 內容的蓄意製作網站，然後引誘使用者檢視該網站。攻擊者也可能利用被駭的網站，或者接受或加載使用者提供之內容或廣告的網站 (透過新增蓄意製作 PDF 內容到這些網站)。只有將 Microsoft Edge 設為預設瀏覽器的 Windows 10 系統會只透過檢視網站而被駭。其他受影響作業系統的瀏覽器不會自動轉譯 PDF 內容，因此攻擊者無從強制使用者檢視由攻擊者操控的內容。而是，攻擊

者必須引誘使用者開啟蓄意製作的 PDF 文件，一般是藉助電子郵件或即時訊息的引誘內容，或電子郵件附件。此更新可修改受影響系統處理記憶體中物件的方式，進而解決此弱點。

(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 92824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/MS16-102
http://www.nessus.org/plugins/index.php?view=single&id=92824
CVE
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3319

二、 [92839]MS16-061：Microsoft Office 的安全性更新 (3177451)

（一）簡要說明

Microsoft OneNote 不當洩漏其記憶體內容時，即存在資訊洩漏弱點。利用此弱點的攻擊者可能使用取得的資訊侵入使用者的電腦或資料。攻擊者可能建立蓄意製作的 OneNote 檔案，然後引誘受害者開啟檔案以利用此弱點。攻擊者必須知道 OneNote 記憶體中的物件位置，攻擊才能成功。(CVE-2016-3315)

當 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。設定為具有較少使用者權限的使用者帳戶所受到的影響，可能會比利用系統管理使用者權限進行操作的使用者帳戶小。

使用者必須以受影響版本的 Microsoft Office 軟體開啟蓄意製作的檔案，攻擊者才有機會利用這些弱點。在電子郵件攻擊案例中，攻擊者可能會傳送蓄意製作的檔案給使用者，然後

引誘使用者開啟該檔案，來利用這些弱點。在網頁式攻擊的案例中，攻擊者可架設一個網站 (或利用會接受或裝載使用者所提供內容的被駭網站)，並在其中包含用來利用這些弱點的蓄意製作檔案。攻擊者並不能強迫使用者造訪網站，而是，攻擊者必須引誘使用者按一下連結，一般是藉助電子郵件的附件或即時訊息，接著再引誘他們開啟蓄意製作的檔案。(CVE-2016-3313、CVE-2016-3316、CVE-2016-3317、CVE-2016-3318)

（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 92839 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/MS16-099
http://www.nessus.org/plugins/index.php?view=single&id= 92839
CVE
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3313
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3315
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3316

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3317
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3318

三、 [92843]Microsoft 圖形元件的安全性更新 (3177393)

（一）簡要說明

當 Windows 字型資源庫不當處理蓄意製作的內嵌字型時，即會存在多個遠端程式碼執行弱點。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。設定為具有較少使用者權限的使用者帳戶所受到的影響，可能會比利用系統管理使用者權限進行操作的使用者帳戶小。

攻擊者有很多方式來利用這些弱點：(CVE-2016-3301、CVE-2016-3303 、 CVE-2016-3304)

- 在網頁型攻擊的案例中，攻擊者可以針對弱點來架設蓄意製作的網站，然後引誘使用者檢視該網站。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訊息或即時訊息中通往攻擊者網站的連結，或開啟經由電子郵件傳送的附件。
- 在檔案共用攻擊的案例中，攻擊者可以提供針對弱點而設計並蓄意製作的文件檔，然後引誘使用者開啟該

文件檔。此安全性更新可以藉由更正 Windows 字型資源庫處理內嵌字型的方式，來解決這些弱點。

（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 92843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/MS16-097
http://www.nessus.org/plugins/index.php?view=single&id=92843
CVE
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3301
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3303
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3304

四、 [92820]MS16-058：Windows IIS 的安全性更新 (3141083)

（一）簡要說明

Microsoft Edge 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，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-2016-3289、CVE-2016-3293、CVE-2016-3319、CVE-2016-3322)

Chakra JavaScript 引擎在處理 Microsoft Edge 記憶體中的物件時，其呈現的方式中存在一個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-2016-3296)

Microsoft Edge 無法正確處理記憶體中物件時，即存在多個資訊洩漏弱點。成功利用這些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-2016-3326、CVE-2016-3327)

當 Microsoft Edge 未正確處理頁面內容時，就會存在多個資訊洩漏弱點，讓攻擊者可以偵測到使用者的電腦上存在著特定檔案。此更新會藉由協助確保在 Microsoft Edge 中正確地驗證頁面內容，進而解決此弱點。(CVE-2016-3329)

（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 ID92820 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/MS16-096
http://www.nessus.org/plugins/index.php?view=single&id=92820
CVE
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3289
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3293

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3296
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3319
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3322
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3329

五、 [92819]Internet Explorer 累積安全性更新 (3177356)

（一）簡要說明

當 Internet Explorer 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。成功利用此弱點的攻擊者可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-2016-3288、CVE-2016-3289、CVE-2016-3290、CVE-2016-3293、CVE-2016-3322)

當 Internet Explorer 未正確處理頁面內容時，就會存在多個資訊洩漏弱點，讓攻擊者可以偵測到使用者的電腦上存在著特定檔案。此更新會藉由協助確保在 Internet Explorer 中正確地驗證頁面內容，進而解決此弱點。(CVE-2016-3321、CVE-2016-3329)

（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 92819 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/MS16-095
http://www.nessus.org/plugins/index.php?view=single&id=92819

CVE
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3288
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3289
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3290
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3293
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3321
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3322
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3326
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3327
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3329