105 年第三季偵測弱點掃描之說明與修補方式

一、 [91013] MS16-064 : Adobe Flash Player 的安全性更新 (3157993)

(一) 簡要說明

當 Windows 主機未安裝修補檔(KB3157993)，可能因下列弱點遭受攻擊：

- 程式碼執行的類型混亂弱點 (CVE-2016-1105、CVE-2016-4117)。
- use-after-free 漏洞，這類漏洞可能導致程式碼執行 (CVE-2016-1097、CVE-2016-1106、CVE-2016-1107、CVE-2016-1108、CVE-2016-1109、CVE-2016-1110、CVE-2016-4108、CVE-2016-4110)。
- 程式碼執行的堆積緩衝區溢出弱點 (CVE-2016-1101)。
- 程式碼執行的緩衝區溢位弱點 (CVE-2016-1103)。
- 記憶體毀損漏洞，這類漏洞可能導致程式碼執行 (CVE-2016-1096、CVE-2016-1098、CVE-2016-1099、CVE-2016-1100、CVE-2016-1102、CVE-2016-1104、CVE-2016-4109、CVE-2016-4111、CVE-2016-4112、CVE-2016-4113、CVE-2016-4114、CVE-2016-4115)。
- 目錄搜尋路徑中用來尋找資源的弱點，此弱點可能導致程式碼執行 (CVE-2016-4116)。

(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 91013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/MS16-064

http://www.nessus.org/plugins/index.php?view=single&id=91013

https://helpx.adobe.com/tw/security/products/flash-player/apsb16-15.html

CVE

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1097

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1098

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1099

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1100

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1101

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1102

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1103

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1104

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1105

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1106

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1107

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1108

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1109

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1110

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1111

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1112

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1113

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1114

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1115

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1116

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1117

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1120

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1121

二、 [91011] MS16-061：Microsoft RPC 的安全性更新 (3155520)

（一）簡要說明

Microsoft Windows 處理蓄意製作的遠端程序呼叫 (RPC) 要求的方式存在遠端執行程式碼弱點。當 RPC 網路資料表現 (NDR) 引擎不當釋放記憶體時，遠端執行程式碼就會發生。成功利用此弱點且通過驗證的攻擊者可執行任意程式碼，並取得受影響之系統的控制權。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。

通過驗證的攻擊者可藉由對受影響主機提出錯誤格式的 RPC 要求利用此弱點。此更新可修改 Microsoft Windows 處理 RPC 訊息的方式，進而解決此弱點。(CVE-2016-0178)

（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 91011 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/MS16-061

http://www.nessus.org/plugins/index.php?view=single&id= 91011

CVE

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0178

三、 [91010] MS16-027：Windows 核心的安全性更新 (3154846)

（一）簡要說明

當 Windows 核心模式驅動程式無法正確處理特定符號連結的剖析時，Microsoft Windows 中即存在權限提高弱點。成功利用此弱點的攻擊者，可能得以存取具特殊權限的登錄機碼，因此提高權限。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。接著，攻擊者便可執行蓄意製作的應用程式來利用此弱點，並取得受影響系統的控制權。此更新可修正 Windows 核心剖析符號連結的方式，進而解決此弱點。 (CVE-2016-0180)

（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 91010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/MS16-060

http://www.nessus.org/plugins/index.php?view=single&id=91010

CVE

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0180

四、 [91008] MS16-058：Windows IIS 的安全性更新 (3141083)

（一）簡要說明

當 Microsoft Windows 無法在載入某些程式庫之前正確地驗證載入時，可能會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上的控制權。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。系統上帳戶使用者權限較低的使用者，其受影響的程度比擁有系統管理權限的使用者要小。

若要利用弱點，攻擊者必須先存取本機系統，並擁有執行惡意應用程式的能力。此安全性更新藉由修正 Windows 在載入程式庫時驗證輸入的方式來解決弱點。 (CVE-2016-0152)

（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 ID91008 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/MS16-058

http://www.nessus.org/plugins/index.php?view=single&id=91008

CVE

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0152

五、 [91007] MS16-024：Windows Shell 的安全性更新 (3156987)

（一）簡要說明

當 Windows Shell 不當處理記憶體中物件時，會存在遠端執行程式碼弱點。成功利用此弱點的攻擊者可執行任意程式碼，並取得受影響之系統的控制權。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。系統上帳戶使用者權限較低的使用者，其受影響的程度比擁有系統管理權限的使用者要小。

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。攻擊者並不能強迫使用者造訪蓄意製作的網站，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。此安全性更新可修正 Windows Shell 處理記憶體中物件的方式，進而解決此弱點。 (CVE-2016-0179)

（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 91007 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/MS16-057

http://www.nessus.org/plugins/index.php?view=single&id=91007

CVE

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0179