TLP:WHITE

金融資安資訊分享與分析中心

漏洞公告-1080717

(Microsoft 發布 2019 年 7 月份系統安全性公告**)**

發行日期：2019 年 7 月 17 日

TLP:WHITE

摘要:

Microsoft 於 2019 年 7 月 9 日(美國時間)發布了多項 Microsoft 安全更新，涵蓋 Microsoft 各類產品，Microsoft 已發布了解決這些漏洞的軟體更新。產品名稱如下。

Microsoft Windows

Internet Explorer

Microsoft Edge

Microsoft Office and Microsoft Office Services and Web Apps

Azure DevOps

Open Source Software

.NET Framework

Azure

SQL Server

ASP.NET

Visual Studio

Microsoft Exchange Server

攻擊者可以利用部分漏洞，取得系統控制權。

根據 CVSS 3.0 分數判斷，其中有 35 項漏洞分數大於 7.0，屬於高風險。

以下將說明高風險漏洞原因、影響及修補方式。

TLP:WHITE

漏洞說明：

項次一：CVE-2019-0785

漏洞名稱：Windows DHCP 伺服器遠端執行程式碼漏洞

概述：

當攻擊者傳送特製封包到 DHCP 容錯移轉伺服器時可造成 Windows Server DHCP 服務存在記憶體損毀漏洞。成功利用漏洞的攻擊者可能會在 DHCP 容錯移轉伺服器上執行任意程式碼，或者造成 DHCP 服務變得沒有回應。

為了利用漏洞，攻擊者可能會傳送特製的封包到 DHCP 伺服器。不過，DHCP 伺服器必須設定為容錯移轉模式，攻擊才會成功。

受影響版本：

如附件，微軟產品影響版本 201907

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：9.8

分析向量：AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

防護方式：

Microsoft 發布了解決此漏洞的軟體更新。沒有解決此漏洞的緩解方法。

相關資訊請參考

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0785

TLP:WHITE

項次二：CVE-2019-0811

漏洞名稱：Windows DNS 伺服器阻斷服務漏洞

概述：

當 Windows DNS 伺服器無法正確地處理 DNS 查詢時，即存在阻斷服務漏洞。成功利用此漏洞的攻擊者可能會造成 DNS 伺服器服務停止回應。

為了利用漏洞，未驗證的攻擊者可能會傳送惡意 DNS 查詢到受影響的伺服器，進而導致阻斷服務。不過，DNS 伺服器必須設定為使用 DNS 分析記錄，攻擊才會成功。

受影響版本：

如附件，微軟產品影響版本 201907

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：7.5

分析向量：AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C

防護方式：

Microsoft 發布了解決此漏洞的軟體更新。

相關資訊請參考

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0811

項次三：CVE-2019-0865

TLP:WHITE

漏洞名稱：SymCrypt 阻斷服務漏洞

概述：

當 SymCrypt 處理特製數位簽章時,存在拒絕服務漏洞。

攻擊者可以通過創建特製連接或消息來利用此漏洞。

受影響版本：

如附件，微軟產品影響版本 201907

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：7.5

分析向量：AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C

防護方式：

Microsoft 發布了解決此漏洞的軟體更新。

相關資訊請參考

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0865

項次四：CVE-2019-0880

漏洞名稱： Microsoft splwow64 權限提高漏洞

概述：

TLP:WHITE

splwow64.exe 處理特定呼叫的方式中，存在本機提權漏洞。成功利用漏洞的攻擊者可能會在受影響的系統上提高權限，從低權限性提高到中權限。

此漏洞本身不會允許執行任意程式碼，然而，如果攻擊者同時利用其他漏洞 (例如遠端執行程式碼漏洞或其他權限提高漏洞)，則可能允許攻擊者執行任意程式碼，當攻擊者嘗試執行程式碼時，就能利用提高的權限。

受影響版本：

如附件，微軟產品影響版本 201907

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：7

分析向量：AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

防護方式：

Microsoft 發布了解決此漏洞的軟體更新。

相關資訊請參考

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0880

項次五：CVE-2019-0887

漏洞名稱：遠端桌面服務遠端執行程式碼漏洞

概述：

TLP:WHITE

當已驗證的攻擊者濫用剪貼簿重新導向時，「遠端桌面服務」(先前稱為終端機服務) 中即存在遠端執行程式碼漏洞。成功利用此漏洞的攻擊者可能會在受害者的系統上執行任意程式碼。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。

為了利用此漏洞，攻擊者必須已經入侵執行「遠端桌面服務」的系統，然後等待受害者系統連線到「遠端桌面服務」。

受影響版本：

如附件，微軟產品影響版本 201907

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：8

分析向量：AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

防護方式：

Microsoft 發布了解決此漏洞的軟體更新。

相關資訊請參考

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0887

項次六：CVE-2019-0999

漏洞名稱：DirectX 權限提高漏洞

概述：

TLP:WHITE

DirectX 不當處理記憶體中的物件時，即存在權限提高漏洞。成功利用此漏洞的攻擊者可能會在核心模式下執行任意程式碼。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。

為了利用此漏洞，攻擊者必須先登入系統。接著，攻擊者可能會執行特製的應用程式來利用漏洞，並取得受影響系統的控制權。

受影響版本：

如附件，微軟產品影響版本 201907

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：7.8

分析向量：AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

防護方式：

Microsoft 發布了解決此漏洞的軟體更新。

相關資訊請參考

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0999

項次七：CVE-2019-1037

漏洞名稱：Windows 錯誤報告權限提高漏洞

概述：

TLP:WHITE

Windows 錯誤報告 (WER) 處理檔案的方式存在提權漏洞。成功利用此漏洞的攻擊者可能會在核心模式下執行任意程式碼。攻擊者接下來將能安裝程式，檢視、變更或刪除資料，或建立具有系統管理員權限的新帳戶。

為了利用漏洞，攻擊者必須先取得受害者系統上未具特殊權限的執行能力。

受影響版本：

如附件，微軟產品影響版本 201907

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：7

分析向量：AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

防護方式：

Microsoft 發布了解決此漏洞的軟體更新。

相關資訊請參考

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-1037

項次八至十一：CVE-2019-1001、CVE-2019-1004、CVE-2019-1056 及 CVE-2019-1059

漏洞名稱：指令碼引擎記憶體損毀漏洞

概述：

TLP:WHITE

指令碼引擎處理 Internet Explorer 記憶體中物件的方式存在遠端執行程式碼漏洞。此漏洞可能會損毀記憶體，使攻擊者有機會在目前使用者的環境中執行任意程式碼。成功利用漏洞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，則成功利用漏洞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，攻擊者可以針對這個經由 Internet Explorer 引起的漏洞來設計並架設特製的網站，然後引誘使用者檢視該網站。攻擊者也可能在主控 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以及接受或存放使用者提供內容或廣告的網站。這些網站可能含有經過特製並利用此漏洞的內容。

受影響版本：

如附件，微軟產品影響版本 201907

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：7.5

分析向量：AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

防護方式：

Microsoft 發布了解決此漏洞的軟體更新。

相關資訊請參考

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-1001

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-1004

TLP:WHITE

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-1056
https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-1059

項次十二：CVE-2019-1063

漏洞名稱：Internet Explorer 記憶體損毀漏洞

概述：

Internet Explorer 不當存取記憶體中的物件時，即存在遠端執行程式碼漏洞。此漏洞可能會損毀記憶體，使攻擊者有機會在目前使用者的內容中執行任意程式碼。成功利用漏洞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。

攻擊者可能會針對經由 Internet Explorer 引起的漏洞來設計並架設特製的網站，然後引誘使用者檢視該網站。攻擊者也可能會新增蓄意製作以利用漏洞的內容，藉此利用受侵害及接受或存放使用者提供內容或廣告的網站。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動作，一般是藉助電子郵件的附件或即時訊息，或是讓使用者開啟經由電子郵件傳送的附件。

受影響版本：

如附件，微軟產品影響版本 201907

影響程度：高

CVSS 向量：

TLP:WHITE

使用版本：CVSS 3.0

分析分數：7.5

分析向量：AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

防護方式：

Microsoft 發布了解決此漏洞的軟體更新。

相關資訊請參考

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-1063

項次十三：CVE-2019-1067

漏洞名稱：Windows 核心權限提高漏洞

概述：

Windows 核心無法正確處理記憶體中的物件時，即存在權限提高漏洞。成功利用此漏洞的攻擊者可能會在核心模式下執行任意程式碼。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。

為了利用此漏洞，攻擊者必須先登入系統。攻擊者便可執行蓄意製作的應用程式，來控制受影響的系統。

此更新會更正 Windows 核心處理記憶體中物件的方式，藉此解決漏洞。

受影響版本：

如附件，微軟產品影響版本 201907

影響程度：高

TLP:WHITE

CVSS 向量：

使用版本：CVSS 3.0

分析分數：7.8

分析向量：AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

防護方式：

Microsoft 發布了解決此漏洞的軟體更新。

相關資訊請參考

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-1067

項次十四：CVE-2019-1082

漏洞名稱：Windows 核心權限提高漏洞

概述：

Microsoft Windows 存在權限提高漏洞，其中具有本機服務權限的特定 dll 可能會競爭放入自訂的 dll。

成功利用此漏洞的攻擊者可能會提高 SYSTEM 的權限。

受影響版本：

如附件，微軟產品影響版本 201907

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：7.7

分析向量：AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L

TLP:WHITE

防護方式：

Microsoft 發布了解決此漏洞的軟體更新。

相關資訊請參考

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-1082

項次十五：CVE-2019-1085

漏洞名稱：Windows WLAN 服務權限提高漏洞

概述：

wlansvc.dll 處理記憶體物件的方式存在權限提高漏洞。成功利用漏洞的攻擊者可能會以提高的權限執行程式碼。

為了利用漏洞，通過本機驗證的攻擊者可能會執行特製的應用程式。

受影響版本：

如附件，微軟產品影響版本 201907

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：7.8

分析向量：AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

防護方式：

Microsoft 發布了解決此漏洞的軟體更新。

相關資訊請參考

TLP:WHITE

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-1085

項次十六至十八：CVE-2019-1086、CVE-2019-1087 及 CVE-2019-1088

漏洞名稱：Windows 音訊服務權限提高漏洞

概述：

Windows 音訊服務中存在提權漏洞。成功利用此漏洞的攻擊者可能會運行具有提升許可權的任意程式碼。

要利用此漏洞,攻擊者可以運行一個特製的應用程式,該應用程式可以利用該漏洞。此漏洞本身不允許運行任意程式碼。但是,此漏洞可以與一個或多個漏洞(例如遠端程式碼執行漏洞和另一個權限提高)結合使用,這些漏洞在運行時可以利用較高的權限。

受影響版本：

如附件，微軟產品影響版本 201907

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：7.8

分析向量：AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

防護方式：

Microsoft 發布了解決此漏洞的軟體更新。

相關資訊請參考

TLP:WHITE

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-1086
https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-1087
https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-1088

項次十九：CVE-2019-1089

漏洞名稱：Windows RPCSS 權限提高漏洞

概述：

當 RPC 服務 Activation Kernel 不正確地處理 RPC 要求時，rpcss.dll 即存在權限提高漏洞。

為了利用此漏洞，經過低層級驗證的攻擊者可能會執行特製的應用程式。

受影響版本：

如附件，微軟產品影響版本 201907

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：7.8

分析向量：AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

防護方式：

Microsoft 發布了解決此漏洞的軟體更新。

相關資訊請參考

TLP:WHITE

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-1089

項次二十：CVE-2019-1090

漏洞名稱：Windows dnsrlvr.dll 權限提高漏洞

概述：

dnsrslvr.dll 處理記憶體物件的方式存在提權漏洞。成功利用漏洞的攻擊者可能會以提高的權限執行程式碼。

為了利用漏洞，在本機通過驗證的攻擊者可能會執行特製的應用程式。

受影響版本：

如附件，微軟產品影響版本 201907

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：7.8

分析向量：AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

防護方式：

Microsoft 發布了解決此漏洞的軟體更新。

相關資訊請參考

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-1090

TLP:WHITE

項次二十一：CVE-2019-1102

漏洞名稱：GDI+ 遠端執行程式碼漏洞

概述：

Windows 圖形裝置介面 (GDI) 處理記憶體中物件的方式存在遠端執行程式碼漏洞。成功利用此漏洞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。設定為具有較小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。

攻擊者可能會採用多種方式來利用漏洞：

在網頁型攻擊的案例中，攻擊者可能會針對漏洞來架設特製的網站，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，而是攻擊者必須引誘使用者採取行動，一般是讓使用者開啟經由電子郵件傳送的附件，或按下電子郵件或即時訊息中的連結。

在檔案共用攻擊的案例中，攻擊者可能會提供針對漏洞而設計並特製的文件檔案，然後引誘使用者開啟該文件檔案。

受影響版本：

如附件，微軟產品影響版本 201907

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：8.4

分析向量：AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

防護方式：

TLP:WHITE

Microsoft 發布了解決此漏洞的軟體更新。

相關資訊請參考

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-1102

項次二十二：CVE-2019-1104

漏洞名稱：Microsoft 瀏覽器記憶體損毀漏洞

概述：

Microsoft 瀏覽器存取記憶體中物件的方式中，存在遠端執行程式碼漏洞。此漏洞可能會損毀記憶體，讓攻擊者能在目前使用者的環境中執行任意程式碼。成功利用漏洞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，攻擊者可能會針對經由 Microsoft 瀏覽器引起的漏洞來設計並架設特製的網站，然後引誘使用者檢視該網站。攻擊者也可能會新增蓄意製作以利用漏洞的內容，藉此利用受侵害及接受或存放使用者提供內容或廣告的網站。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動作，一般是藉助電子郵件的附件或即時訊息，或是讓他們開啟經由電子郵件傳送的附件。

受影響版本：

如附件，微軟產品影響版本 201907

影響程度：高

TLP:WHITE

CVSS 向量：

使用版本：CVSS 3.0

分析分數：7.5

分析向量：AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

防護方式：

Microsoft 發布了解決此漏洞的軟體更新。

相關資訊請參考

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-1104

項次二十三至三十二：CVE-2019-1117、CVE-2019-1118、CVE-2019-1119、CVE-2019-1120、CVE-2019-1121、CVE-2019-1122、CVE-2019-1123、CVE-2019-1124、CVE-2019-1127 及 CVE-2019-1128

漏洞名稱：DirectWrite 遠端執行程式碼漏洞

概述：

DirectWrite 處理記憶體物件的方式中，存在遠端執行程式碼漏洞。成功利用此漏洞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。

有多種攻擊者可以利用此漏洞的方式，例如引誘使用者開啟特製的文件，或引誘他們造訪未受信任的網頁。

TLP:WHITE

受影響版本：

如附件，微軟產品影響版本 201907

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：7.8

分析向量：AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

防護方式：

Microsoft 發布了解決此漏洞的軟體更新。

相關資訊請參考

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-1117
https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-1118
https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-1119
https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-1120
https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-1121
https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-1122
https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-1123
https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-1124

TLP:WHITE

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-1127
https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-1128

項次三十三及三十四：CVE-2019-1129 及 CVE-2019-1130

漏洞名稱：Windows 權限提高漏洞

概述：

當 Windows AppX 部署服務 (AppXSVC) 不正確地處理永久連結時，即存在權限提高漏洞。成功利用此漏洞的攻擊者可能會使用已提高權限的內容執行處理程序。攻擊者便可藉機安裝程式；檢視、變更或刪除資料。

為了利用此漏洞，攻擊者必須先登入系統。接著，攻擊者可能會執行特製的應用程式來利用漏洞，並取得具此漏洞系統的控制權。

受影響版本：

如附件，微軟產品影響版本 201907

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：7.8

分析向量：AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

防護方式：

Microsoft 發布了解決此漏洞的軟體更新。

相關資訊請參考

TLP:WHITE

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-1129
https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-1130

項次三十五：CVE-2019-1132

漏洞名稱：Windows 權限提高漏洞

概述：

Win32k 元件無法正確處理記憶體中的物件時，Windows 中即存在權限提高漏洞。成功利用此漏洞的攻擊者可能會在核心模式下執行任意程式碼。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。

為了利用此漏洞，攻擊者必須先登入系統。接著，攻擊者可能會執行特製的應用程式來利用漏洞，並取得受影響系統的控制權。

受影響版本：

如附件，微軟產品影響版本 201907

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：7.8

分析向量：AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

防護方式：

Microsoft 發布了解決此漏洞的軟體更新。

TLP:WHITE

相關資訊請參考

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-1132

參考連結：

1. Microsoft

https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/48293f19-d662-e911-a98e-000d3a33c573