TLP:WHITE

# 金融資安資訊分享與分析中心

# 漏洞公告-1080516

**(Microsoft** 發布 2019 年 5 月份系統安全性公告**)**

**發行日期：2019 年 5 月 16 日**

TLP:WHITE

**摘要:**

Microsoft 於 2019 年 5 月 14 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。

Adobe Flash Player

Microsoft Windows

Internet Explorer

Microsoft Edge

Microsoft Office and Microsoft Office Services and Web Apps

Team Foundation Server

Visual Studio

Azure DevOps Server

SQL Server

.NET Framework

.NET Core

ASP.NET Core

ChakraCore

Online Services

Azure

TLP:WHITE

NuGet

Skype for Android

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 30 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。

其中編號為 CVE-2019-0708 的遠端桌面服務之遠端執行程式碼漏洞，

CVSS 3.0 分數為 9.8，屬於重大漏洞，請盡速修補。

**漏洞說明：**

**項次一：CVE-2019-0707**

**漏洞名稱：Windows NDIS 提權漏洞**

**概述：**

當 ndis.sys 無法在將記憶體複製到緩衝區之前先檢查緩衝區的長度時，其存在「網路驅動程式介面規格」(NDIS) 提權漏洞。

在本機攻擊的案例中，攻擊者可能會執行特製的應用程式，藉此利用漏洞提高攻擊者的權限等級。成功利用此漏洞的攻擊者可能會在已提權的環境中執行處理程序。然而，攻擊者必須先取得本機系統的存取權，並擁有執行惡意應用程式的能力，才能夠利用此漏洞。

**受影響版本：**

如附件，微軟產品影響版本 201905

TLP:WHITE

**影響程度：高**

**CVSS 向量：**

使用版本：CVSS 3.0

**分析分數：**7.0

**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。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-2019-0707

## 項次二：CVE-2019-0708

**漏洞名稱：遠端桌面服務遠端執行程式碼漏洞**

**概述：**

「遠端桌面服務」存在遠端執行程式碼漏洞，其於當未經驗證的攻擊者使用 RDP 連線到目標系統並傳送特製的請求。此漏洞已預先通過認證，且不需要使用者互動。成功利用此漏洞的攻擊者可能會在目標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，攻擊者必須透過 RDP 對目標系統的「遠端桌面服務」傳送特製的請求。

**受影響版本：**

如附件，微軟產品影響版本 201905

**影響程度：高**

TLP:WHITE

**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。

或可採用下列緩解方法。

1. 在運行 Windows 7，Windows Server 2008 和 Windows Server 2008 R2 的受維護支援版本的系統上啟用網路級別身份驗證（Network Level Authentication, NLA）

透過啟用網路級別身份驗證，阻止未經身份認證的攻擊者利用此漏洞。啟用 NLA 後，攻擊者首先需要使用目標系統上的有效帳戶對遠端桌面服務進行身份認證，然後才能利用此漏洞。

2.在企業邊界防火牆處關閉 TCP 連接埠 3389 對外服務

TCP 連接埠 3389 用於啟動與受影響組件的連接。在網路邊界防火牆關閉此連接埠對外服務，有助於保護防火牆之後的系統免於漏洞遭利用。這有助於免受來自企業外部的攻擊。但是，系統仍可能易受來自於企業環境內的攻擊。

**相關資訊請參考**

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0708

## 項次三：CVE-2019-0725

TLP:WHITE

## 漏洞名稱：Windows DHCP 伺服器遠端執行程式碼漏洞

**概述：**

Windows Server DHCP 服務在處理特製封包時，存在記憶體損毀漏洞。成功利用漏洞的攻擊者可在 DHCP 伺服器上執行任意程式碼。

未經認證的遠端攻擊者可以傳送特製的封包到受此漏洞影響的 DHCP 伺服器來利用此漏洞。

**受影響版本：**

如附件，微軟產品影響版本 201905

**影響程度：高**

**CVSS 向量：**

使用版本：CVSS 3.0

分析分數：8.1

分析向量：AV:N/AC:H/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-2019-0725

## 項次四：CVE-2019-0734

## 漏洞名稱：Windows 提權漏洞

**概述：**

TLP:WHITE

Microsoft Windows 存在提全漏洞，當中間人攻擊可以順利解碼並取代使用 Kerberos 的認證要求，進而允許攻擊者被驗證為系統管理員身分。

**受影響版本：**

如附件，微軟產品影響版本 201905

**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。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-2019-0734

## 項次五：CVE-2019-0863

## 漏洞名稱：Windows 錯誤報告提權漏洞

**概述：**

Windows 錯誤報告 (Windows Error Reporting , 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以在 Kernel 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。

TLP:WHITE

為了利用漏洞，攻擊者必須先取得受害系統上無特權的執行能力。

**受影響版本：**

如附件，微軟產品影響版本 201905

**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。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-2019-0863

## 項次六：CVE-2019-0881

## 漏洞名稱：Windows 核心提權漏洞

**概述：**

Windows Kernel 未能適當處理機碼列舉時，即存在提權漏洞。成功利用漏洞的攻擊者可能會在目標系統上獲得權限提升。

經過本機認證的攻擊者可能會執行特製的應用程式，藉此利用此漏洞。

**受影響版本：**

如附件，微軟產品影響版本 201905

TLP:WHITE

**影響程度：高**

**CVSS 向量：**

使用版本：CVSS 3.0

分析分數：8.8

分析向量：AV:N/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。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-2019-0881

## 項次七至九：CVE-2019-0884、CVE-2019-0911、CVE-2019-0918

### 漏洞名稱：指令碼引擎記憶體損毀漏洞

**概述：**

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

TLP:WHITE

可能在主控瀏覽器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」。攻擊者也可能利用遭入侵的網站及接受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 201905

**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。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-2019-0884
https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0911
https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0918

## 項次十：CVE-2019-0885

## 漏洞名稱：Windows OLE 遠端執行程式碼漏洞

**概述：**

TLP:WHITE

當 Microsoft Windows OLE 無法正確地驗證使用者輸入時，即存在遠端執行程式碼漏洞。攻擊者可能會利用漏洞來執行惡意程式碼。

為了利用漏洞，攻擊者必須引誘使用者開啟特製的檔案或程式，進而造成 Windows 執行任意程式碼。

**受影響版本：**

如附件，微軟產品影響版本 201905

**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。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-2019-0885

## 項次十一至二十三：CVE-2019-0889、CVE-2019-0890、CVE-2019-0891、CVE-2019-0893、CVE-2019-0894、CVE-2019-0895、CVE-2019-0896、CVE-2019-0897、CVE-

TLP:WHITE

## 2019-0898、CVE-2019-0899、CVE-2019-0900、CVE-2019-0901、CVE-2019-0902

### 漏洞名稱：Jet 資料庫引擎遠端執行程式碼漏洞

**概述：**

當 Windows Jet 資料庫引擎不正確地處理記憶體中的物件時，即存在遠端執行程式碼漏洞。成功利用此漏洞的攻擊者可在受害者的系統上執行任意程式碼。

攻擊者可引誘受害者開啟特製的檔案，藉此利用漏洞。

**受影響版本：**

如附件，微軟產品影響版本 201905

**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。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-2019-0889

TLP:WHITE

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0890

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0891

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0893

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0894

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0895

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0896

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0897

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0898

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0899

TLP:WHITE

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0900

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0901

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0902

## 項次二十四：CVE-2019-0892

## 漏洞名稱：Win32k 提權漏洞

**概述：**

Win32k 元件無法正確處理記憶體中的物件時，Windows 中即存在提權漏洞。成功利用此漏洞的攻擊者可在 Kernel 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 201905

**影響程度：高**

**CVSS 向量：**

使用版本：CVSS 3.0

TLP:WHITE

**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。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-2019-0892

## 項次二十五：CVE-2019-0903

## 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中，存在遠端執行程式碼漏洞。成功利用此漏洞的攻擊者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。設定為具有較小使用者權限的使用者帳戶所受到的影響，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。

TLP:WHITE

**受影響版本：**

如附件，微軟產品影響版本 201905

**影響程度：高**

**CVSS 向量：**

使用版本：CVSS 3.0

分析分數：8.8

分析向量：AV:N/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。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-2019-0903

## 項次二十六：CVE-2019-0929

## 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。

TLP:WHITE

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利用漏洞特製的內容，藉此利用遭入侵的網站及接受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立即訊息，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 201905

**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

**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-2019-0929

## 項次二十七：CVE-2019-0931

## 漏洞名稱：Windows 存放服務提權漏洞

**概述：**

當存放服務不當處理檔案操作時，存在權限提高漏洞。成功利用這個漏洞的攻擊者可以在受害者系統上提權。

若要利用該漏洞，攻擊者首先必須操作受害者系統，然後運行經特殊設計的應用程式。

**受影響版本：**

如附件，微軟產品影響版本 201905

**影響程度：高**

**CVSS 向量：**

使用版本：CVSS 3.0

分析分數：7.0

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。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-2019-0931

## 項次二十八：CVE-2019-0936

## 漏洞名稱：Windows 提權漏洞

**概述：**

TLP:WHITE

當 Windows 無法正確地處理特定符號連結時，Microsoft Windows 中即存在提權漏洞。成功利用此漏洞的攻擊者可能會將特定項目設定為以較高等級執行，進而提高權限。

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 201905

**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。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-2019-0936

## 項次二十九：CVE-2019-0940

## 漏洞名稱：Microsoft 瀏覽器記憶體損毀漏洞

**概述：**

TLP:WHITE

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特製以利用漏洞的內容，藉此利用遭入侵的網站及接受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立即訊息，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 201905

**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: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。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-2019-0940

TLP:WHITE

## 項次三十：CVE-2019-0995

## 漏洞名稱：Internet Explorer 安全性功能繞過漏洞

**概述：**

當 urlmon.dll 不正確地處理特定 Web 標記查詢時，即存在安全性功能繞過漏洞。此漏洞會允許 Internet Explorer 繞過 Web 標記警告，或對以特定方式下載或建立的檔案所做的限制。

在網頁式攻擊的案例中，攻擊者必須裝載利用漏洞設計的惡意檔案，然後引誘使用者下載惡意檔案並在 Internet Explorer 中開啟檔案。

**受影響版本：**

如附件，微軟產品影響版本 201905

**影響程度：高**

**CVSS 向量：**

使用版本：CVSS 3.0

分析分數：7.3

分析向量：AV:L/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。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-2019-0995

TLP:WHITE

**參考連結：**

1. Microsoft

https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/e5989c8b-7046-e911-a98e-000d3a33a34d