TLP:WHITE

金融資安資訊分享與分析中心

漏洞公告-1080918

(Microsoft 發布 2019 年 9 月份系統安全性公告**)**

發行日期：2019 年 9 月 18 日

TLP:WHITE

摘要:

Microsoft 於 2019 年 9 月 10 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 (EdgeHTML-based)

ChakraCore

Microsoft Office and Microsoft Office Services and Web Apps

Adobe Flash Player

Microsoft Lync

Visual Studio

Microsoft Exchange Server

.NET Framework

Microsoft Yammer

.NET Core

ASP.NET

Team Foundation Server

Project Rome

TLP:WHITE

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 31 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。

漏洞說明：

項次一至四：CVE-2019-0787、CVE-2019-0788、CVE-2019-1290 及 CVE-2019-1291

漏洞名稱：遠端桌面用戶端遠端執行程式碼漏洞

概述：

當使用者連線到惡意伺服器時，表示 Windows 遠端桌面用戶端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連線用戶端的電腦上執行任意程式碼。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，攻擊者可能必須擁有伺服器的控制權，然後引誘使用者連線到伺服器。攻擊者無法強迫使用者連線到惡意伺服器，而是必須透過社交工程、DNS 破壞或使用中間人攻擊(MITM) 技巧，引誘使用者連線。此外，攻擊者可能也會入侵合法伺服器，在伺服器上裝載惡意程式碼，然後等待使用者連線。

受影響版本：

如附件，微軟產品影響版本 201909

TLP:WHITE

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-2019-0787

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-0788

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1290

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1291

項次五及六：CVE-2019-1208 及 CVE-2019-1236

漏洞名稱：VBScript 遠端執行程式碼漏洞

概述：

VBScript 引擎處理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。成功利用此漏洞的攻擊者可以取得與目前使用者相同的使用者權

TLP:WHITE

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以取得具此漏洞系統的控制權。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。

在網頁型攻擊案例中，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」。攻擊者也可能利用遭入侵以及接受或裝載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 201909

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-2019-1208

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1236

TLP:WHITE

項次七：CVE-2019-1214

漏洞名稱：Windows 通用記錄檔系統驅動程式權限提高漏洞

概述：

當 Windows 通用記錄檔系統 (CLFS)的驅動程式不正確地處理記憶體中物件時，即存在權限提高漏洞。成功利用此漏洞的攻擊者可能會在已提高權限的內容中執行處理程序。

為了利用漏洞，攻擊者必須先登入系統，然後執行特製的應用程式，以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 201909

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

TLP:WHITE

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1214

項次八：CVE-2019-1215

漏洞名稱：Windows 權限提高漏洞

概述：

ws2ifsl.sys (Winsock) 處理記憶體物件的方式中，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，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 201909

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-2019-1215

TLP:WHITE

項次九：CVE-2019-1221

漏洞名稱：Windows 權限提高漏洞

概述：

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具此漏洞系統的控制權。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 201909

TLP:WHITE

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-2019-1221

項次十：CVE-2019-1232

漏洞名稱：診斷集線器標準收集器服務權限提高漏洞

概述：

當「診斷集線器標準收集器服務」不正確地模擬特定檔案操作時，即存在權限提高漏洞。成功利用此漏洞的攻擊者可能會取得提高的權限。

若攻擊者擁有具此漏洞系統的未經授權存取權，則可能會利用此漏洞。

受影響版本：

如附件，微軟產品影響版本 201909

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：7.8

TLP:WHITE

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-2019-1232

項次十一：CVE-2019-1235

漏洞名稱：診斷集線器標準收集器服務權限提高漏洞

概述：

當 Text Service Framework (TSF) 伺服器處理序無法驗證接收到的輸入或命令的來源時，表示 Windows TSF 存在權限提高漏洞。成功利用此漏洞的攻擊者可能會插入命令或讀取透過惡意輸入法 (IME) 傳送的輸入。這只會對已安裝 IME 的系統造成影響。

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 201909

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

TLP:WHITE

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-2019-1235

項次十二至二十 ：CVE-2019-1240、CVE-2019-1241、CVE-2019-1242、CVE-2019-1243、CVE-2019-1246、CVE-2019-1247、CVE-2019-1248、CVE-2019-1249 及 CVE-2019-1250

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能會在受害者的系統上執行任意程式碼。

攻擊者可能會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 201909

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

TLP:WHITE

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-2019-1240

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1241

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1242

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1243

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1246

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1247

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1248

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1249

TLP:WHITE

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1250

項次二十一：CVE-2019-1253

漏洞名稱：Windows 權限提高漏洞

概述：

當 Windows AppX 部署伺服器不正確地處理接合時，即存在權限提高漏洞。

為了利用此漏洞，攻擊者必須先取得在受害者系統上執行作業的權限。接著，攻擊者可能會執行特製的應用程式以提升權限。

受影響版本：

如附件，微軟產品影響版本 201909

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-2019-1253

TLP:WHITE

項次二十二及二十三：CVE-2019-1256 及 CVE-2019-1285

漏洞名稱：Win32k 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 201909

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-2019-1256

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1285

TLP:WHITE

項次二十四：CVE-2019-1267

漏洞名稱：Microsoft Compatibility Appraiser 權限提高漏洞

概述：

Microsoft Compatibility Appraiser 存在權限提高漏洞，其中具有本機權限的設定檔容易受到符號連結攻擊和永久連結攻擊。成功利用此漏洞的攻擊者可能會在提高權限的環境中執行處理程序。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 201909

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:C/C:L/I:H/A:L/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-2019-1267

TLP:WHITE

項次二十五：CVE-2019-1271

漏洞名稱：Windows Media 權限提高漏洞

概述：

hdAudio.sys 存在權限提高漏洞，可能會導致超出範圍的寫入。成功利用此漏洞的攻擊者可能會在提高權限的內容中執行處理程序。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。攻擊者便可執行特製的應用程式，來控制具此漏洞的系統。

受影響版本：

如附件，微軟產品影響版本 201909

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:C/C:H/I:L/A:L/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-2019-1271

TLP:WHITE

項次二十六：CVE-2019-1273

漏洞名稱：Active Directory 同盟服務 XSS 漏洞

概述：

當 Active Directory 同盟服務 (ADFS) 無法正確地處理特定錯誤訊息時，即存在跨網站指令碼 (XSS) 漏洞。已驗證的攻擊者可能會傳送特製的要求給具此漏洞的 ADFS 伺服器，藉此利用漏洞。
接著，成功利用漏洞的攻擊者可能會在具此漏洞的系統上執行跨網站指令碼攻擊，並在目前使用者的安全性內容中執行指令碼。這些攻擊可能會允許攻擊者讀取攻擊者無權讀取的內容、使用受害者的身分代表使用者在 ADFS 網站上執行變更權限及刪除內容等動作，以及將惡意內容插入使用者的瀏覽器。

受影響版本：

如附件，微軟產品影響版本 201909

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：8.2

分析向量：AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N/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-2019-1273

TLP:WHITE

項次二十七：CVE-2019-1277

漏洞名稱：Windows 音訊服務權限提高漏洞

概述：

當 Windows 音訊服務處理格式錯誤的參數時，即存在權限提高漏洞。當用來搭配其他漏洞時，成功利用漏洞的攻擊者可能會以提高的權限執行任意程式碼。

為了利用漏洞，攻擊者可能會在本機執行特製的應用程式。此漏洞本身不會允許執行任意程式碼。但是，此漏洞可能用來搭配一個或多個漏洞 (例如，遠端執行程式碼漏洞和另一個權限提高漏洞)，而那些漏洞可能會在執行時利用權限提高漏洞。

受影響版本：

如附件，微軟產品影響版本 201909

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-2019-1277

TLP:WHITE

項次二十八：CVE-2019-1278

漏洞名稱：Windows 權限提高漏洞

概述：

當 Active Directory 同盟服務 (ADFS) 無法正確地處理特定錯誤訊息時，即存在跨網站指令碼 (XSS) 漏洞。已驗證的攻擊者可能會傳送特製的要求給具此漏洞的 ADFS 伺服器，藉此利用漏洞。
接著，成功利用漏洞的攻擊者可能會在具此漏洞的系統上執行跨網站指令碼攻擊，並在目前使用者的安全性內容中執行指令碼。這些攻擊可能會允許攻擊者讀取攻擊者無權讀取的內容、使用受害者的身分代表使用者在 ADFS 網站上執行變更權限及刪除內容等動作，以及將惡意內容插入使用者的瀏覽器。

受影響版本：

如附件，微軟產品影響版本 201909

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-2019-1278

TLP:WHITE

項次二十九：CVE-2019-1284

漏洞名稱：DirectX 權限提高漏洞

概述：

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 201909

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-2019-1284

TLP:WHITE

項次三十：CVE-2019-1287

漏洞名稱：Windows 網路連線助理權限提高漏洞

概述：

「Windows 網路連線助理」處理記憶體中物件的方式中，存在權限提高漏洞。成功利用漏洞的攻擊者會以提高的權限執行程式碼。

在本機通過驗證的攻擊者可執行特製的應用程式以利用此漏洞。

受影響版本：

如附件，微軟產品影響版本 201909

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-2019-1287

項次三十一：CVE-2019-1289

TLP:WHITE

漏洞名稱：Windows Update 傳遞最佳化權限提高漏洞

概述：

當 Windows Update 傳遞最佳化(Delivery Optimization)無法正確強制執行檔案共用權限時，即存在權限提高漏洞。成功利用漏洞的攻擊者會覆寫需要較高權限 (比攻擊者原有的權限還高) 的檔案。
為了利用此漏洞，攻擊者必須登入系統。然後，攻擊者可能會建立傳遞最佳化工作，以利用漏洞。

受影響版本：

如附件，微軟產品影響版本 201909

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。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-2019-1289

參考連結：

1. Microsoft

TLP:WHITE

https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/24f46f0a-489c-e911-a994-000d3a33c573