TLP:WHITE

金融資安資訊分享與分析中心

漏洞公告-1081120

(Microsoft 發布 2019 年 11 月份系統安全性公告**)**

發行日期：2019 年 11 月 20 日

TLP:WHITE

摘要:

Microsoft 於 2019 年 11 月 12 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

Open Source Software

Microsoft Exchange Server

Visual Studio

Azure Stack

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 38 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：

項次一及二：CVE-2019-0719、CVE-2019-0721

漏洞名稱：Hyper-V 遠端執行程式碼漏洞

概述：

當主機伺服器上的 Windows Hyper-V 網路交換器無法在客體作業系統上正確驗證已驗證使用者的輸入時，表示存在遠端執行程式碼漏洞。為了利用此漏洞，攻擊者可能會在客體作業系統上執行特製的應用程式，造成 Hyper-V 主機作業系統執行任意程式碼。

成功利用漏洞的攻擊者可能會在主機作業系統上執行任意程式碼。

受影響版本：

如附件，微軟產品影響版本 201911

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:H/PR:H/UI:N/S:C/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-2019-0719

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-0721

項次三：CVE-2019-1370

TLP:WHITE

漏洞名稱：Open Enclave SDK 資訊洩漏漏洞

概述：

當受影響的 Open Enclave SDK 版本不當處理記憶體中的物件時，即存在資訊洩漏漏洞。成功利用此漏洞的攻擊者可能會取得 Enclave 中儲存的資訊。

為了利用此漏洞，攻擊者必須成功入侵執行 Enclave 的主機應用程式。攻擊者接著會將 Enclave 作為樞紐，不須與使用者有任何互動，即可利用此漏洞。

受影響版本：

如附件，微軟產品影響版本 201911

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:L/I:L/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-2019-1370

項次四至六：CVE-2019-1379、CVE-2019-1383 及 CVE-2019-1417

漏洞名稱：Windows 資料共用服務權限提高漏洞

概述：

TLP:WHITE

當「Windows 資料共用服務」不正確地處理檔案操作時，即存在權限提高漏洞。成功利用此漏洞的攻擊者可能會在已提高權限的內容中執行處理程序。

攻擊者可能會在受害者的系統上執行特製的應用程式，藉此利用漏洞。

受影響版本：

如附件，微軟產品影響版本 201911

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-2019-1379

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1383

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1417

項次七：CVE-2019-1380

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，存在本機權限提高漏洞。成功利用漏洞的攻擊者可能會在具此漏洞的系統上提高權限，由低完整性提高到中完整性。

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 201911

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-2019-1380

項次八：CVE-2019-1382

漏洞名稱：Microsoft ActiveX 安裝程式服務權限提高漏洞

概述：

當 ActiveX 安裝程式服務允許在未經適當驗證的情況下存取檔案時，即存在權限提高漏洞。成功利用此漏洞的攻擊者可能會存取未經授權的檔案。

TLP:WHITE

為了利用此漏洞，已驗證的攻擊者可能會在受害者系統中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 201911

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-2019-1382

項次九：CVE-2019-1384

漏洞名稱：Microsoft Windows 安全性功能略過漏洞

概述：

NETLOGON 訊息能夠取得階段作業金鑰和簽署郵件的位置，即存在安全性功能略過漏洞。

為了利用此漏洞，攻擊者可能會傳送特製的驗證要求。成功利用此漏洞的攻擊者可使用原始的使用者權限存取其他機器。

受影響版本：

如附件，微軟產品影響版本 201911

影響程度：高

TLP:WHITE

CVSS 向量：

使用版本：CVSS 3.0

分析分數：8.5

分析向量：AV:N/AC:H/PR:L/UI:N/S:C/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-2019-1384

項次十：CVE-2019-1385

漏洞名稱：Windows AppX 部署擴充功能權限提高漏洞

概述：

當 Windows AppX 部署擴充功能不當執行權限管理，而導致可存取系統檔案時，即存在權限提高漏洞。

為了利用此漏洞，已驗證的攻擊者必須執行特製的應用程來提高權限。

受影響版本：

如附件，微軟產品影響版本 201911

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。

TLP:WHITE

相關資訊請參考
https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1385

項次十一：CVE-2019-1388

漏洞名稱：Windows 憑證對話方塊權限提高漏洞

概述：

當 Windows 憑證對話方塊無法正確地強制執行使用者權限時，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。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 201911

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-2019-1388

TLP:WHITE

項次十二至十四：CVE-2019-1389、CVE-2019-1397 及 CVE-2019-1398

漏洞名稱：Windows Hyper-V 遠端執行程式碼漏洞

概述：

當主機伺服器上的 Windows Hyper-V 無法在客體作業系統上正確地驗證已驗證使用者的輸入時，即存在遠端執行程式碼漏洞。為了利用此漏洞，攻擊者可能會在客體作業系統上執行特製的應用程式，造成 Hyper-V 主機作業系統執行任意程式碼。

成功利用漏洞的攻擊者可能會在主機作業系統上執行任意程式碼。

受影響版本：

如附件，微軟產品影響版本 201911

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：7.6

分析向量：AV:A/AC:H/PR:H/UI:N/S:C/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-2019-1389

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1397

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1398

TLP:WHITE

項次十五：CVE-2019-1390

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 201911

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。

TLP:WHITE

相關資訊請參考
https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1390

項次十六：CVE-2019-1392

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。攻擊者便可執行特製的應用程式，來控制受影響的系統。

受影響版本：

如附件，微軟產品影響版本 201911

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-2019-1392

TLP:WHITE

項次十七至二十一：CVE-2019-1393、CVE-2019-1394、CVE-2019-1395、CVE-2019-1396、CVE-2019-1408

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 201911

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-2019-1393

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1394

TLP:WHITE

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1395
https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1396
https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1408

項次二十二：CVE-2019-1405

漏洞名稱：Windows UPnP 服務權限提高漏洞

概述：

當 Windows 通用隨插即用 (UPnP) 服務允許不當建立 COM 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以提高的系統權限執行任意程式碼。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。
若要利用此漏洞，攻擊者必須登入受影響的系統，並執行特製的指令碼或應用程式。

受影響版本：

如附件，微軟產品影響版本 201911

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：

TLP:WHITE

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-2019-1405

項次二十三至二十七：CVE-2019-1407、CVE-2019-1433、CVE-2019-1435、CVE-2019-1437、CVE-2019-1438

漏洞名稱：Windows 圖形元件權限提高漏洞

概述：

Windows 圖形元件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已提高權限的環境中執行處理程序。在本機攻擊的案例中，攻擊者可能會執行特製的應用程式，藉此利用漏洞以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 201911

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：7.8(CVE-2019-1407)

7(CVE-2019-1433、CVE-2019-1435、CVE-2019-1437、CVE-2019-1438)

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 (CVE-2019-1407)

AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C(CVE-2019-1433、CVE-2019-1435、CVE-2019-1437、CVE-2019-1438)

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-2019-1407

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1433

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1435

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1437

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1438

項次二十八：CVE-2019-1415

漏洞名稱：Windows Installer 權限提高漏洞

概述：

由於 Windows Installer 處理某些文件系統操作的方式，Windows Installer 中存在一個特權提升漏洞。

要利用此漏洞，攻擊者需具受害者系統的非特權執行權限。成功利用此漏洞後，攻擊者即具有特權可執行任意程式碼。然後，攻擊者可能會安裝程序。查看，更改或刪除資料；或創建具有完全用戶權限的新帳戶。

受影響版本：

如附件，微軟產品影響版本 201911

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: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-2019-1415

項次二十九：CVE-2019-1416

漏洞名稱：適用於 Linux 的 Windows 子系統權限提高漏洞

概述：

由於適用於 Linux 的 Windows 子系統出現競爭條件，表示存在權限提高漏洞。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 201911

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。

TLP:WHITE

相關資訊請參考

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1416

項次三十及三十一：CVE-2019-1419 及 CVE-2019-1456

漏洞名稱：OpenType 字型剖析遠端執行程式碼漏洞

概述：

當 Windows Adobe Type Manager 程式庫不當處理特製的 OpenType 字型時，Microsoft Windows 中即存在遠端執行程式碼漏洞。對於 Windows 10 以外的所有系統，成功利用漏洞的攻擊者可能會從遠端執行程式碼。對於執行 Windows 10 的系統，成功利用這項漏洞的攻擊者可以在包含限制權限和功能的 AppContainer 沙箱內容中執行程式碼。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。

攻擊者有多種方式可以來利用此漏洞，例如引誘使用者開啟特製的文件，或引誘使用者造訪包含特製的內嵌 OpenType 字型的網頁。

受影響版本：

如附件，微軟產品影響版本 201911

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。

TLP:WHITE

相關資訊請參考
https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1419
https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1456

項次三十二：CVE-2019-1420

漏洞名稱：Windows 權限提高漏洞

概述：

dssvc.dll 處理允許在安全的位置覆寫或建立檔案的檔案建立方式中，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 201911

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-2019-1420

TLP:WHITE

項次三十三：CVE-2019-1422

漏洞名稱：Windows 權限提高漏洞

概述：

phlpsvc.dll 處理允許覆寫檔案的檔案建立方式中，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 201911

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-2019-1422

項次三十四：CVE-2019-1423

漏洞名稱：Windows 權限提高漏洞

概述：

TLP:WHITE

StartTileData.dll 在受保護位置建立檔案的處理方式中，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 201911

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-2019-1423

項次三十五：CVE-2019-1424

漏洞名稱：NetLogon 安全性功能略過漏洞

概述：

當 Windows Netlogon 不當處理安全通訊管道時，即存在安全性功能略過漏洞。成功利用漏洞的攻擊者可能會將連線降級，以允許進一步修改傳輸。

為了利用此漏洞，攻擊者要針對目標流量發動備妥主動式中間人攻擊。

受影響版本：

如附件，微軟產品影響版本 201911

TLP:WHITE

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-2019-1424

項次三十六：CVE-2019-1429

漏洞名稱：指令碼引擎記憶體損毀漏洞

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

侵害的網站、接受或存放使用者提供之內容或廣告的網站。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 201911

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-2019-1429

項次三十七：CVE-2019-1430

漏洞名稱：Microsoft Windows 媒體基礎遠端執行程式碼漏洞

概述：

當 Windows 媒體基礎不當剖析特製的 QuickTime 媒體檔案時，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取得與本機使用者相同的使用者權限。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。

TLP:WHITE

為了利用漏洞，攻擊者必須將特別特製的 QuickTime 檔案傳送給使用者，並引誘他們開啟檔案。開啟時，惡意的 QuickTime 檔案會在目標系統執行攻擊者選擇的程式碼。

受影響版本：

如附件，微軟產品影響版本 201911

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-2019-1430

項次三十八：CVE-2019-1434

漏洞名稱：Win32k 權限提高漏洞

概述：

當 Windows 核心模式驅動程式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。

TLP:WHITE

受影響版本：

如附件，微軟產品影響版本 201911

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-2019-1434

參考連結：

1. Microsoft

https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/164aa83e-499c-e911-a994-000d3a33c573