TLP:WHITE

金融資安資訊分享與分析中心

漏洞公告-1080820

(Microsoft 發布 2019 年 8 月份系統安全性公告**)**

發行日期：2019 年 8 月 20 日

TLP:WHITE

摘要:

Microsoft 於 2019 年 8 月 13 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

ChakraCore

Microsoft Office and Microsoft Office Services and Web Apps

Visual Studio

Online Services

Active Directory

Microsoft Dynamics

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 50 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-2019-0720

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 201908

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-2019-0720

項次二：CVE-2019-0736

TLP:WHITE

漏洞名稱：Windows DHCP 用戶端遠端執行程式碼漏洞

概述：

當攻擊者傳送特製的 DHCP 回應到用戶端時，表示 Windows DHCP 用戶端存在記憶體損毀漏洞。成功利用漏洞的攻擊者可能會在用戶端電腦上執行任意程式碼。

為了利用漏洞，攻擊者可能會傳送特製的 DHCP 回應給用戶端。

受影響版本：

如附件，微軟產品影響版本 201908

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-2019-0736

項次三：CVE-2019-0965

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 201908

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-2019-0965

項次四：CVE-2019-1057

漏洞名稱：MS XML 遠端執行程式碼漏洞

概述：

當 Microsoft XML Core Services MSXML 剖析器處理使用者輸入時，即存在遠端執行程式碼漏洞。成功利用漏洞的攻擊者可能會從遠端執行惡意程式碼，以取得使用者系統的控制權。

為了利用漏洞，攻擊者可能會架設特製的網站，以透過網頁瀏覽器叫用 MSXML。然而，攻擊者並無法強迫使用者造訪這類網站，而是引誘使用者自行前往。一般的做法是設法讓使用者按一下電子郵件訊息或即時訊息

中通往攻擊者網站的連結。當 Internet Explorer 剖析 XML 內容時，攻擊者可能會從遠端執行惡意程式碼，以控制使用者的系統。

受影響版本：

如附件，微軟產品影響版本 201908

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-2019-1057

項次五：CVE-2019-1133

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。

TLP:WHITE

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 201908

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-2019-1133

項次六至十一：CVE-2019-1144、CVE-2019-1145、CVE-2019-1149、CVE-2019-1150、CVE-2019-1151、CVE-2019-1152

漏洞名稱：Microsoft 圖形遠端執行程式碼漏洞

概述：

TLP:WHITE

當 Windows 字型資源庫不當處理特製的內嵌字型時，即存在遠端執行程式碼漏洞。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。設定為具有較小使用者權限的使用者帳戶所受到的影響，會比以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，而是必須引誘使用者自行前往。一般的做法是設法讓使用者按一下電子郵件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。

在檔案共用攻擊的案例中，攻擊者可能會提供特製並設計利用漏洞的文件檔案，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 201908

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。

相關資訊請參考

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1144

TLP:WHITE

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1145
https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1149
https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1150
https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1151
https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1152

項次十二至十六：CVE-2019-1146、CVE-2019-1147、CVE-2019-1155、CVE-2019-1156、CVE-2019-1157

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 201908

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: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-2019-1146
https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1147
https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1155
https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1156
https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1157

項次十七及十八：CVE-2019-1159 及 CVE-2019-1164

漏洞名稱：Windows 核心提權漏洞

概述：

Windows 核心無法正確處理記憶體中的物件時，即存在提權漏洞。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：

TLP:WHITE

如附件，微軟產品影響版本 201908

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-2019-1159

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1164

項次十九：CVE-2019-1162

漏洞名稱：Windows ALPC 提權漏洞

概述：

當 Windows 不正確地處理對 Advanced Local Procedure Call (ALPC) 的呼叫時，即存在提權漏洞。

成功利用此漏洞的攻擊者可能會在本機系統的安全性內容中執行任意程式碼。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：

TLP:WHITE

如附件，微軟產品影響版本 201908

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:F/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-2019-1162

項次二十：CVE-2019-1168

漏洞名稱：Microsoft Windows p2pimsvc 提權漏洞

概述：

當成功利用漏洞的攻擊者可能以提高的權限執行任意程式碼時，即表示 p2pimsvc 服務存在提權漏洞。

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 201908

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: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-2019-1168

項次二十一：CVE-2019-1169

漏洞名稱：Win32k 提權漏洞

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 201908

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：

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-2019-1169

項次二十二：CVE-2019-1170

漏洞名稱：Windows NTFS 提權漏洞

概述：

當沙箱化處理程序建立重新分析點，以允許沙箱逸出時，即存在提權漏洞。成功利用漏洞的攻擊者可能會在受影響的系統上利用沙箱逃逸提高權限。

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 201908

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：7.9

分析向量：AV:L/AC:L/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。

相關資訊請參考

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1170

TLP:WHITE

項次二十三及二十四：CVE-2019-1173 及 CVE-2019-1174

漏洞名稱：Windows 提權漏洞

概述：

PsmServiceExtHost.dll 處理記憶體物件的方式中，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 201908

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-2019-1173

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1174

項次二十五：CVE-2019-1175

漏洞名稱：Windows 提權漏洞

TLP:WHITE

概述：

psmsrv.dll 處理記憶體物件的方式中，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 201908

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-2019-1175

項次二十六：CVE-2019-1176

漏洞名稱：DirectX 提權漏洞

概述：

DirectX 不當處理記憶體中的物件時，即存在提權漏洞。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 201908

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-2019-1176

項次二十七：CVE-2019-1177

漏洞名稱：Windows 提權漏洞

概述：

rpcss.dll 處理記憶體物件的方式中，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 201908

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：7

TLP:WHITE

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-2019-1177

項次二十八：CVE-2019-1178

漏洞名稱：Windows 提權漏洞

概述：

ssdpsrv.dll 處理記憶體物件的方式中，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 201908

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

TLP:WHITE

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1178

項次二十九及三十：CVE-2019-1180 及 CVE-2019-1186

漏洞名稱：Windows 提權漏洞

概述：

wcmsvc.dll 處理記憶體物件的方式中，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 201908

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-2019-1180

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1186

TLP:WHITE

項次三十一至三十四：CVE-2019-1181、CVE-2019-1182、CVE-2019-1222 及 CVE-2019-1226

漏洞名稱：遠端桌面服務遠端執行程式碼漏洞

概述：

當未驗證的攻擊者使用 RDP 連線到目標系統並傳送特製的要求時，「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。此漏洞是預先驗證，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」傳送特製的要求。

受影響版本：

如附件，微軟產品影響版本 201908

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。

相關資訊請參考

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1181

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1182

TLP:WHITE

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1222
https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1226

項次三十五：CVE-2019-1183

漏洞名稱：Windows VBScript 引擎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，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 201908

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

TLP:WHITE

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-2019-1183

項次三十六：CVE-2019-1188

漏洞名稱：LNK 遠端執行程式碼漏洞

概述：

如果處理 .LNK 檔案，Microsoft Windows 即存在遠端執行程式碼漏洞，可能會允許攻擊者遠端執行程式碼。

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。

攻擊者可能會向使用者顯示抽取式磁碟機或遠端共用，其中包含惡意 .LNK 檔案和關聯的惡意二進位檔案。當使用者在 Windows 檔案總管中開啟這個磁碟機 (或遠端共用)，或者任何其他應用程式剖析 .LNK 檔案時，惡意二進位檔案將會在目標系統上執行攻擊者所選的程式碼。

受影響版本：

如附件，微軟產品影響版本 201908

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

TLP:WHITE

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-2019-1188

項次三十七：CVE-2019-1190

漏洞名稱：Windows 映像提權漏洞

概述：

Windows 核心映像處理記憶體中物件的方式中，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 201908

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-2019-1190

項次三十八：CVE-2019-1194

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 201908

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

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-2019-1194

項次三十九：CVE-2019-1206

漏洞名稱：Windows DHCP 伺服器阻斷服務漏洞

概述：

當攻擊者傳送特製的封包到 DHCP 容錯移轉伺服器時，表示 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 201908

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

TLP:WHITE

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1206

項次四十至四十一：CVE-2019-1212 至 CVE-2019-1213

漏洞名稱：Windows DHCP 伺服器阻斷服務漏洞

概述：

在處理特製的封包時，表示 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造成 DHCP 伺服器服務停止回應。

為了利用漏洞，未驗證的遠端攻擊者可能會傳送特製的封包到受影響的 DHCP 伺服器。

受影響版本：

如附件，微軟產品影響版本 201908

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。

相關資訊請參考

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1212

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1213

TLP:WHITE

項次四十二：CVE-2019-1223

漏洞名稱：Windows 遠端桌面通訊協定 (RDP) 阻斷服務漏洞

概述：

當攻擊者使用遠端桌面通訊協定 (RDP) 連線到目標系統並傳送特製的要求時，RDP 中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目標系統上的 RDP 服務停止回應。

為了利用此漏洞，攻擊者必須對提供「遠端桌面通訊協定」(RDP) 服務的伺服器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 201908

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-2019-1223

項次四十三及四十四：CVE-2019-1224 及 CVE-2019-1225

漏洞名稱：遠端桌面通訊協定伺服器資訊洩漏漏洞

TLP:WHITE

概述：

當 Windows RDP 伺服器不正確地洩漏其記憶體中的內容時，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資訊，進一步入侵系統。

為了利用此漏洞，攻擊者必須從遠端連線到受影響的系統，並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 201908

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-2019-1224

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1225

項次四十五：CVE-2019-9506

漏洞名稱：藍芽加密金鑰交涉漏洞

概述：

TLP:WHITE

Microsoft 已知存在於任何 BR/EDR 藍芽裝置之硬體規格層級的藍芽 BR/EDR (基本速率/延伸資料速率，又稱為 "Bluetooth Classic") 金鑰交涉漏洞。攻擊者可能能夠進行交涉，將提供的金鑰長度從 Entropy 最大的 16 位元組降低成 1 位元組。

為了利用此漏洞，攻擊者需要特殊化硬體，並且可能會因為使用中的藍芽裝置範圍而受到限制。透過使用這個特殊化設備，攻擊者必須離得夠近才能通訊並干擾以無線方式進行的合法傳輸。

受影響版本：

如附件，微軟產品影響版本 201908

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：9.3

分析向量：AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N/E:U/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-2019-9506

項次四十六至五十：CVE-2019-9511、CVE-2019-9512、CVE-2019-9513、CVE-2019-9514、CVE-2019-9518

漏洞名稱：HTTP/2 伺服器阻斷服務漏洞

概述：

TLP:WHITE

當 HTTP.sys 不正確地剖析特製的 HTTP/2 要求時，HTTP/2 通訊協定堆疊 (HTTP.sys) 中即存在阻斷服務漏洞。成功利用漏洞的攻擊者可能會造成阻斷服務的情形，使目標系統停止回應。

為了利用此漏洞，未驗證的攻擊者可能會傳送特製的 HTTP 封包至目標系統，導致受影響的系統停止回應。

受影響版本：

如附件，微軟產品影響版本 201908

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-2019-9511

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-9512

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-9513

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-9514

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-9518

TLP:WHITE

參考連結：

1. Microsoft

https://portal.msrc.microsoft.com/zh-tw/security-guidance/releasenotedetail/312890cc-3673-e911-a991-000d3a33a34d