TLP:WHITE

金融資安資訊分享與分析中心

漏洞公告-1081017

(Microsoft 發布 2019 年 10 月份系統安全性公告**)**

發行日期：2019 年 10 月 17 日

TLP:WHITE

摘要:

Microsoft 於 2019 年 10 月 8 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

SQL Server Management Studio

Open Source Software

Microsoft Dynamics 365

Windows Update Assistant

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 24 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-2019-1238 及 CVE-2019-1239

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 201910

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。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-2019-1238

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1239

項次三：CVE-2019-1311

漏洞名稱：Windows Imaging API 遠端執行程式碼漏洞

概述：

當 Windows Imaging API 無法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。此漏洞可能會損毀記憶體，讓攻擊者能在目前使用者的內容中執行任意程式碼。

為了利用漏洞，攻擊者必須引誘使用者開啟特製的.WIM 檔案。

受影響版本：

如附件，微軟產品影響版本 201910

影響程度：高

CVSS 向量：

TLP:WHITE

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-2019-1311

項次四及五：CVE-2019-1315 及 CVE-2019-1339

漏洞名稱：Windows 錯誤報告管理員權限提高漏洞

概述：

當 Windows 錯誤報告管理員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覆寫目標檔案，進而造成權限提高的狀態。

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 201910

影響程度：高

CVSS 向量：

TLP:WHITE

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-2019-1315

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1339

項次六：CVE-2019-1316

漏洞名稱：Microsoft Windows 安裝程式權限提高漏洞

概述：

當 Microsoft Windows 安裝程式無法正確地處理權限時，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 201910

TLP:WHITE

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:N/S:C/C:L/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-2019-1316

項次七：CVE-2019-1318

漏洞名稱：Microsoft Windows 安裝程式權限提高漏洞

概述：

當「傳輸層安全性」(TLS) 存取非 Extended Master Secret (EMS) 工作階段時，即存在偽造內容漏洞。成功利用此漏洞的攻擊者可能會取得未經授權的資訊的存取權。

為了利用漏洞，攻擊者必須先進行中間人攻擊。

受影響版本：

如附件，微軟產品影響版本 201910

影響程度：高

CVSS 向量：

TLP:WHITE

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/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-2019-1318

項次八至十：CVE-2019-1319、CVE-2019-1320 及 CVE-2019-1322

漏洞名稱：Windows 錯誤報告權限提高漏洞

概述：

當 Windows 錯誤報告 (WER) 處理並執行檔案時，WER 即存在權限提高漏洞。如果攻擊者能成功利用漏洞，漏洞可能會允許權限提高。

成功利用漏洞的攻擊者可能會取得更高的權限，以存取敏感資訊和系統功能。為了利用漏洞，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 201910

影響程度：高

CVSS 向量：

TLP:WHITE

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-2019-1319

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1320

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1322

項次十一及十二：CVE-2019-1323 及 CVE-2019-1336

漏洞名稱：Microsoft Windows Update 用戶端權限提高漏洞

概述：

當 Microsoft Windows Update 用戶端無法正確地處理權限時，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 201910

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: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-2019-1323

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1336

項次十三：CVE-2019-1326

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。

TLP:WHITE

受影響版本：

如附件，微軟產品影響版本 201910

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。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-2019-1326

項次十四：CVE-2019-1333

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 201910

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-2019-1333

項次十五：CVE-2019-1340

漏洞名稱：Microsoft Windows 權限提高漏洞

概述：

Windows AppX 部署伺服器允許在任意位置建立檔案，因此存在權限提高漏洞。

為了利用漏洞，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 201910

TLP:WHITE

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。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-2019-1340

項次十六：CVE-2019-1341

漏洞名稱：Windows 電源服務權限提高漏洞

概述：

當電源服務的 umpo.dll 不正確地處理登錄還原機碼功能時，即存在權限提高漏洞。成功利用此漏洞的攻擊者可能會刪除目標登錄機碼，進而造成權限提高的狀態。

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 201910

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。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-2019-1341

項次十七：CVE-2019-1342

漏洞名稱：Windows 錯誤報告管理員權限提高漏洞

概述：

當 Windows 錯誤報告管理員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覆寫目標檔案，進而造成權限提高的狀態。

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 201910

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

TLP:WHITE

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-2019-1342

項次十八及十九：CVE-2019-1358 及 CVE-2019-1359

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 201910

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

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-2019-1358

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1359

項次二十及二十一：CVE-2019-1362 及 CVE-2019-1364

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 201910

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。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-2019-1362

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1364

項次二十二：CVE-2019-1365

漏洞名稱：Microsoft IIS Server 權限提高漏洞

概述：

當 Microsoft IIS Server 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，即存在權限提高漏洞。

成功利用此漏洞的攻擊者可能會允許使用者所執行的不具權限功能，以便在 NT AUTHORITY\system 內容中執行程式碼，進而逸出沙箱。

受影響版本：

如附件，微軟產品影響版本 201910

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：7.5

TLP:WHITE

分析向量：AV:N/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-2019-1365

項次二十三：CVE-2019-1367

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，然後藉由傳送電子郵件等方式引誘使用者檢視該網站。

受影響版本：

如附件，微軟產品影響版本 201910

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: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-2019-1367

項次二十四：CVE-2019-1371

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。

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特製以利用漏洞的內容，藉此利用受侵害及接受或存放使用者提供之內容或廣告的網站。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。

TLP:WHITE

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 201910

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-2019-1371

參考連結：

1. Microsoft

https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/28ef0a64-489c-e911-a994-000d3a33c573