TLP:WHITE

金融資安資訊分享與分析中心

漏洞公告-1081220

(Microsoft 發布 2019 年 12 月份系統安全性公告)

發行日期：2019 年 12 月 20 日

TLP:WHITE

摘要:

Microsoft 於 2019 年 12 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 Office、Microsoft Office Services 和 Web Apps

SQL Server

Visual Studio

Skype for Business

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 10 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：CVE-2019-1453

TLP:WHITE

漏洞名稱：Windows 遠端桌面協定 (RDP) 拒絕服務漏洞

概述：

遠端桌面協定 (RDP)存在一個拒絕服務漏洞，當攻擊到目標系統使用 RDP 連接並發送特製的請求。攻擊者成功利用此漏洞可能導致 RDP 服務目標系統停止回應。

要利用此漏洞，攻擊者需要對一個提供遠端桌面協定 (RDP) 服務伺服器執行一個特製的應用程式。

受影響版本：

如附件，微軟產品影響版本 201912

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-2019-1453

項次二：CVE-2019-1458

漏洞名稱：Microsoft 圖形元件權限提高漏洞

概述：

TLP:WHITE

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。

如果要利用此漏洞，攻擊者首先必須登入系統。接著，攻擊者便可執行特製的應用程式來利用此漏洞，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 201912

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-2019-1458

項次三：CVE-2019-1468

漏洞名稱：Win32k 圖形遠端執行程式碼漏洞

概述：

TLP:WHITE

一個遠端代碼執行漏洞存在時 Windows 字體庫無法正確處理特製的嵌入字體。攻擊者成功利用此漏洞可以控制具此漏洞的系統。攻擊者可隨後安裝程式;查看、更改或刪除資料;或者建立擁有完整使用者權限的新帳戶。在系統上其帳戶被設定為擁有較小使用者權限的使用者，其所受影響會比設定為具有管理使用者許可權的使用者小。

攻擊者可使用多種方法利用此漏洞。

在 web 的攻擊情形中，攻擊者可以設立一個特製的網站，旨在利用此漏洞，然後誘使使用者查看該網站。攻擊者沒有任何辦法強迫使用者查看攻擊者控制的內容。相反，攻擊者必須說服使用者採取行動，通常是讓使用者按一下在電子郵件訊息的一個連結或需要使用者連到攻擊者的網站，透過即時訊息或開啟電子郵件中的附件。

在檔案共用的攻擊情形中，攻擊者可以提供一個利用此漏洞的特製檔案，然後誘使使用者打開該檔案。

受影響版本：

受影響版本：

如附件，微軟產品影響版本 201912

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：8.4

分析向量：AV:L/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

TLP:WHITE

https://portal.msrc.microsoft.com/zh-TW/security-guidance/advisory/CVE-2019-1468

項次四：CVE-2019-1471

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 無法在虛擬主機作業系統上正確驗證已驗證的使用者的輸入時，即存在遠端執行程式碼漏洞。為了利用此漏洞，攻擊者可能會在虛擬主機作業系統上執行特製的應用程式，造成 Hyper-V 主機作業系統可執行任意程式碼。

成功利用此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 201912

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:L/AC:L/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-2019-1471

TLP:WHITE

項次五：CVE-2019-1476

漏洞名稱：Windows 權限提高漏洞

概述：

當 Windows AppX 部署服務 (AppXSVC) 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使用已提高權限的內容執行處理程序。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 201912

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-2019-1476

TLP:WHITE

項次六：CVE-2019-1477

漏洞名稱：Windows 印表機服務權限提高漏洞

概述：

當 Windows 印表機服務無法在載入印表機驅動程式時正確地驗證檔案路徑，即存在權限提高弱點。已驗證且成功利用此弱點的攻擊者可能會以提高的系統權限執行任意程式碼。

為了利用此弱點，攻擊者必須先登入系統。接著，攻擊者可能會執行蓄意製作的應用程式來利用弱點，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 201912

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-2019-1477

項次七：CVE-2019-1478

TLP:WHITE

漏洞名稱：Windows COM 伺服器權限提高漏洞

概述：

當 Windows 不正確地處理 COM 物件建立時，即存在權限提高弱點。成功利用弱點的攻擊者可能會以提高的權限執行任意程式碼。

為了利用此弱點，攻擊者必須先登入系統。接著，攻擊者可能會執行蓄意製作的應用程式來利用弱點，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 201912

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-2019-1478

項次八：CVE-2019-1483

漏洞名稱：Windows 權限提高漏洞

概述：

TLP:WHITE

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

為了利用此弱點，攻擊者必須先取得在受害者系統上執行作業的權限。接著，攻擊者可能會執行蓄意製作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 201912

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-2019-1483

項次九：CVE-2019-1484

漏洞名稱：Windows OLE 遠端執行程式碼漏洞

概述：

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弱點。攻擊者可能會利用弱點來執行惡意程式碼。

為了利用弱點，攻擊者必須引誘使用者開啟蓄意製作的檔案或程式，進而造成 Windows 執行任意程式碼。

TLP:WHITE

受影響版本：

如附件，微軟產品影響版本 201912

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-2019-1484

項次十：CVE-2019-1485

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弱點。此弱點可能會損毀記憶體，使攻擊者有機會在目前使用者的內容中執行任意程式碼。成功利用此弱點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，則成功利用弱點的攻擊者可以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

在網頁型攻擊案例中，攻擊者可能會針對經由 Internet Explorer 引起的弱點來設計並架設蓄意製作的網站，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的網站，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蓄意製作並利用此弱點的內容。

受影響版本：

如附件，微軟產品影響版本 201912

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-2019-1485

參考連結：

1. Microsoft

https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2019-Dec