TLP:WHITE

金融資安資訊分享與分析中心

弱點公告-1080111-1

(Microsoft 發布 2019 年 1 月份系統安全性公告**)**

發行日期：2019 年 1 月 11 日

TLP:WHITE

摘要:

Microsoft 於 2019 年 1 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。

Internet Explorer

Microsoft Edge

Microsoft Windows

Microsoft Office and Microsoft Office Services and Web Apps

ChakraCore

.NET Framework

ASP.NET

Microsoft Exchange Server

Microsoft Visual Studio

Adobe Flash Player

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 23 項漏洞分數大於 7.0，屬於高風險。

TLP:WHITE

以下將說明高風險漏洞原因、影響及修補方式。

漏洞說明：

項次一至十一：CVE-2019-0538、CVE-2019-0575、CVE-2019-0576、CVE-2019-0577、CVE-2019-0578、CVE-2019-0579、CVE-2019-0580、CVE-2019-0581、CVE-2019-0582、CVE-2019-0583 及 CVE-2019-0584

漏洞名稱：Jet 資料庫引擎遠端執行程式碼弱點

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弱點。成功利用此弱點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，藉此利用弱點。

受影響版本：

如附件，微軟產品影響版本

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：7.8（原廠自評）

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：

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-2019-0538

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0575

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0576

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0577

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0578

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0579

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0580

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0581

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0582

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0583

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0584

項次十二：CVE-2019-0541

TLP:WHITE

漏洞名稱：Internet Explorer 遠端執行程式碼弱點

概述：

Internet Explorer (IE) 未正確地驗證輸入內容，存在遠端執行程式碼弱點。攻擊者可能會在目前使用者的環境中執行任意程式碼。成功利用弱點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，則成功利用弱點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 html 編輯攻擊案例中，攻擊者可能會引誘使用者編輯設計來利用弱點的特製檔案。

受影響版本：

如附件，微軟產品影響版本

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：7.5（原廠自評）

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-2019-0541

TLP:WHITE

項次十三：CVE-2019-0543

漏洞名稱：Microsoft Windows 權限提高弱點

概述：

Microsoft JET 資料庫引擎中存在緩衝區溢位漏洞，可能會允許在受影響的系統上執行遠端程式碼。攻擊者成功利用此漏洞的可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。系統中帳戶設定為具有較低使用者權限的使用者，其所受到的影響可能會比具系統管理員權限的使用者小。

使用者必須以受影響版本的 Microsoft Windows 開啟特製的 Excel 檔案，攻擊者才有機會利用漏洞。在電子郵件攻擊案例中，攻擊者可能會傳送特製的 Excel 檔案給使用者，然後引誘使用者開啟該檔案，藉此利用漏洞。

受影響版本：

如附件，微軟產品影響版本

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：7.8（原廠自評）

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

TLP:WHITE

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0543

項次十四：CVE-2019-0547

漏洞名稱：Windows DHCP 用戶端遠端執行程式碼弱點

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弱點。成功利用弱點的攻擊者可能會在用戶端電腦上執行任意程式碼。

為了利用弱點，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

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：9.8（原廠自評）

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

TLP:WHITE

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0547

項次十五及十六：CVE-2019-0550 及 CVE-2019-0551

漏洞名稱：Windows Hyper-V 遠端執行程式碼弱點

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弱點。為了利用此弱點，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。

成功利用弱點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

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：7.6（原廠自評）

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

TLP:WHITE

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0550

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0551

項次十七：CVE-2019-0552

漏洞名稱：Windows COM 權限提高弱點

概述：

Windows COM 桌面代理程式中存在權限提高弱點。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。

為了利用弱點，攻擊者可能會執行特製以利用弱點的應用程式。此弱點本身不會允許執行任意程式碼。但是，此弱點可能用來搭配一個或多個弱點(例如，遠端執行程式碼弱點和另一個權限提高弱點)，而那些弱點可能會在執行時利用權限提高弱點。

受影響版本：

如附件，微軟產品影響版本

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：7.0（原廠自評）

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：

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-2019-0552

項次十八：CVE-2019-0555

漏洞名稱：Microsoft XmlDocument 權限提高弱點

概述：

Microsoft XmlDocument 類別存在權限提高弱點，此弱點可能會允許攻擊者自瀏覽器的 AppContainer 沙箱中逃逸。成功利用此弱點的攻擊者可能會獲得提高的權限，並突破 Edge AppContainer 沙箱。

此弱點本身不會允許執行任意程式碼。但是，此弱點可能搭配一個或多個弱點 (例如，遠端執行程式碼弱點和另一個權限提高弱點) 使用，以便在執行時利用權限提高弱點。

受影響版本：

如附件，微軟產品影響版本

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：7.0（原廠自評）

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。

TLP:WHITE

相關資訊請參考

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0555

項次十九：CVE-2019-0570

漏洞名稱：Windows 執行階段權限提高弱點

概述：

當 Windows 執行階段不正確地處理記憶體中的物件時，即存在權限提高弱點。成功利用此弱點的攻擊者可能會在已提高權限的內容中執行任意程式碼。

攻擊者可能會在受害者的系統上執行特製的應用程式，藉此利用弱點。

受影響版本：

如附件，微軟產品影響版本

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：7.8（原廠自評）

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

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-2019-0570

項次二十至二十三：CVE-2019-0571、CVE-2019-0572、CVE-2019-0573 及 CVE-2019-0574

漏洞名稱：Windows 資料共用服務權限提高弱點

概述：

當「Windows 資料共用服務」不正確地處理檔案操作時，即存在權限提高弱點。成功利用此弱點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，藉此利用弱點。

受影響版本：

如附件，微軟產品影響版本

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：7.8（原廠自評）

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

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-2019-0571

TLP:WHITE

https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0572
https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0573
https://portal.msrc.microsoft.com/zh-tw/security-guidance/advisory/CVE-2019-0574

參考連結：

1. Microsoft

https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/b4384b95-e6d2-e811-a983-000d3a33c573