INFORMATION
數聯資安
SECURITY SERVICE

重大更新，微軟釋出更新修補安全性漏洞

總頁數，：9 頁（含封面及附件）

文件編號：X-099

機密等級：□機密□密■一般

中華民國 109 年 12 月 15 日

目　　錄

壹、 相關訊息 3
貳、 訊息深入探討 4
一、 微軟安全性更新 4
參、 影響範圍 6
肆、 防護及修補建議 7
伍、 參考資料 8

圖 目 錄

圖 1　微軟 20201211 安全性更新 4

壹、 相關訊息

2020/12/11 微軟釋出更新包，修補了 58 個安全漏洞，當中有 9 個被列為重大（Critical）漏洞，

本週資安預警通報針對相關廠商於重大修補日推出的修補包及相關漏洞進行介紹。

貳、 訊息深入探討

一、 微軟安全性更新

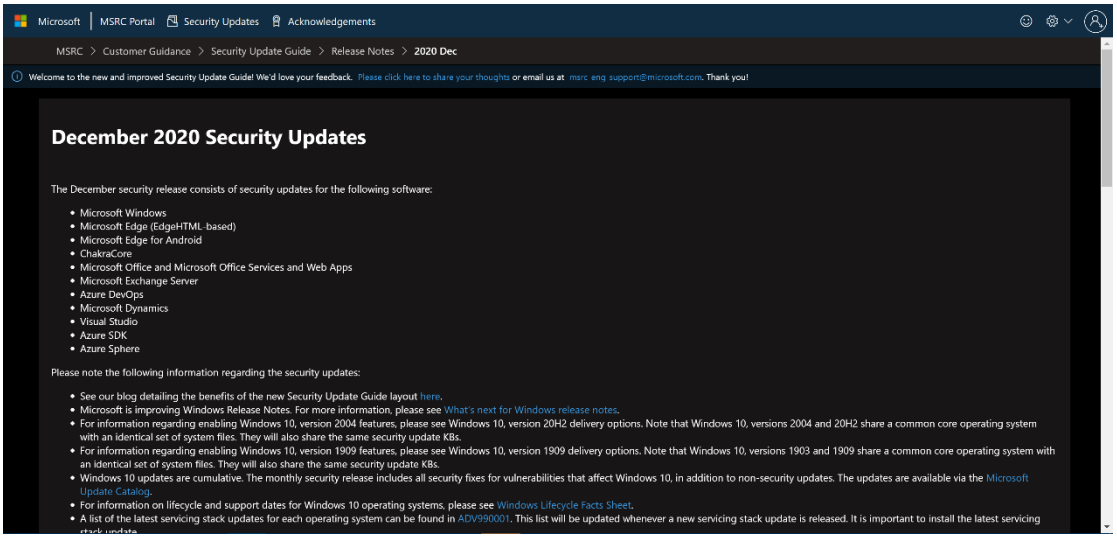

圖1　*微軟 20201211 安全性更新*

微軟於 20201211 的 Patch Tuesday 釋出針對 Microsoft Windows、Edge、ChakraCore、Microsoft Office 和 Office Services、Web Apps、Exchange Server、Azure DevOps、Microsoft Dynamics、Visual Studio、Azure SDK 的安全更新補丁。

在本周漏洞修補的 58 個 CVE 安全漏洞修復補丁，嚴重風險的 CVE 共 9 項、高風險的 CVE 共 3 項、中風險的 CVE 共 46 項，下文將針對值得注目的 CVE 漏洞進行介紹。

- CVE-2020-17132　Exchange 任意程式碼遠端執行漏洞

Microsoft 並未說明此漏洞的詳細利用方式，但說明攻擊者需要進行身份驗證才能利用此漏洞進行攻擊。這代表當管理者的信箱被攻擊者竊取時，攻擊者可以接管整個 Exchange 伺服器。

- CVE-2020-17121　SharePoint 任意程式碼遠端執行漏洞

此漏洞允許經過身份驗證的用戶在 SharePoint Web 應用程式服務中在受影響的伺服器上執行任意的.NET 程式碼

- CVE-2020-17095　Hyper-V 任意程式碼遠端執行漏洞

此漏洞允許攻擊者透過傳送 特定的 vSMB 封包並從 Hyper-V 虛擬機中傳送至 Hyper-V 主機內，藉此提權。

- CVE-2020-16996　Kerberos 安全功能繞過漏洞

此漏洞 Microsoft 並無提供相關的細節，僅發布有關管理 RBCD /受保護用戶更改的部署指南。

參、影響範圍

12 月份釋出更新包含適用於下列軟體的安全性更新:

- Microsoft Windows
- Microsoft Windows Server
- Microsoft Exchange Server
- Microsoft SharePoint Server
- Microsoft Azure
- Microsoft Edge (以 Chromium 為基礎) 的 IE 模式
- Microsoft Team Foundation Server
- Microsoft Office
- Microsoft Outlook
- ChakraCore

肆、 防護及修補建議

- Micosoft 所推出的修補漏洞有許多重大風險等級漏洞，目前已有相關 POC 釋出，還請客戶多多提防並更新。
- 建議系統管理者進行更新測試，確認公司測試環境、系統未有異常狀況再佈署更新，或暫緩更新 7-35 天，待微軟釋出修補更新。

伍、 參考資料

- https://www.thezdi.com/blog/2020/12/8/the-december-2020-security-update-review
- https://www.ithome.com.tw/news/141606