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-100

機密等級：□機密□密■一般

中華民國 110 年 01 月 15 日

目錄

圖 目 錄

壹、 相關訊息

2021/01/12 微軟釋出更新包，修補了 83 個安全漏洞，當中有 10 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

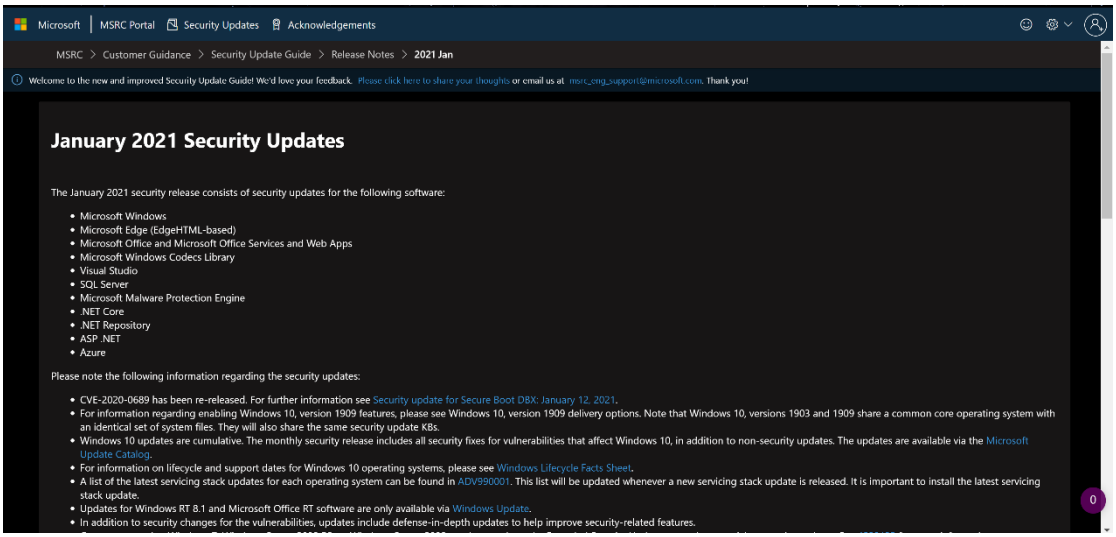

圖1　*微軟 20210112 安全性更新*

微軟於 20210112 的 Patch Tuesday 釋出針對 Microsoft Windows、Microsoft Edge (EdgeHTML-based)、Microsoft Office and Microsoft Office Services and Web Apps、Microsoft Windows Codecs Library、Visual Studio、SQL Server、Microsoft Malware Protection Engine、.NET Core、.NET Repository、ASP .NET、Azure 的安全更新程式。

在本周漏洞修補的 83 個 CVE 安全漏洞修復補丁，嚴重風險的 CVE 共 10 項、高風險的 CVE 共 73 項，下文將針對值得注目的 CVE 漏洞進行介紹。

- CVE-2021-1647 Microsoft Defender 遠端任意程式碼執行漏洞

Microsoft 沒有說明此 Microsoft Defender 漏洞的相關技術細節，僅說明相關安全更新程式將透過自動更新發布，並表示目前以偵測到有駭客正掃描利用此漏洞。

- CVE-2021-1648 Microsoft splwow64 提權漏洞

此漏洞為先前安全更新程式的更新錯誤，先前的安全更新程式引入了一個檢查輸入字串指針的功能，但是這樣做導致 Out-of-Bounds（OOB）Read 錯誤。

- CVE-2021-1677 Azure Active Directory Pod 身份驗證繞過漏洞

此漏洞為 Azure Active Directory（AAD）Pod 允許使用者帳號在分配 Pod 角色時以 Kubernete 集群的方式存在。當 Pod 被以此方式分內後，該 Pod 可以訪問 Azure Instance Metadata Service（IMDS）節點並獲取相關 token。

- CVE-2021-1674 Windows 遠端桌面 Protocol 的核心安全功能繞過漏洞

此漏洞並無相關的詳細介紹，僅猜測此為繞過了 RDP Core 中的某些安全功能。

參、影響範圍

01 月份釋出更新包含適用於下列軟體的安全性更新:

- Microsoft Windows
- Microsoft Edge (EdgeHTML-based)
- Microsoft Office and Microsoft Office Services and Web Apps
- Microsoft Windows Codecs Library
- Visual Studio
- SQL Server
- Microsoft Malware Protection Engine
- .NET Core
- .NET Repository
- ASP .NET
- Azure

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://msrc.microsoft.com/update-guide/releaseNote/2021-Jan
- https://www.thezdi.com/blog/2021/1/12/the-january-2021-security-update-review