附件 3

110年9月13日～10月12日資安攻擊及漏洞警訊，請各校資安聯絡人確認並進行更新：

一、【漏洞預警】蘋果iOS系統存在安全漏洞(CVE-2021-30858、30860)，允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新。

(一) [內容說明:]

轉發 國家資安資訊分享與分析中心 資安訊息警訊 NISAC-ANA-202109-0846

研究人員發現蘋果相關作業系統存在安全漏洞(CVE-2021-30858、30860)，攻擊者可誘騙使用者開啟惡意PDF文件或網頁，利用這些漏洞遠端執行任意程式碼。

情資分享等級: WHITE(情資內容為可公開揭露之資訊)

(二) [影響平台:]

1.CVE-2021-30858：

■ macOS Catalina 與 macOS Mojave：Safari 14.1.2(不含)以前版本

■ macOS Big Sur：macOS Big Sur 11.6(不含)以前版本

■ iPhone 6s(含)以上機型與 iPod touch 第 7 代：iOS 14.8(不含)以前版本

■ iPad Pro(所有機型)、iPad Air 2、iPad 5(含)以上機型及 iPad mini 4(含)以上機型：iPadOS 14.8(不含)以前版本

2.CVE-2021-30860：

■ macOS Catalina：Security Update 2021-005 Catalina(不含)以前版本

■ macOS Big Sur：macOS Big Sur 11.6(不含)以前版本

■ Apple Watch Series 3(含)以上機型：watchOS 7.6.2(不含)以前版本

■ iPhone 6s(含)以上機型與 iPod touch 第 7 代：iOS 14.8(不含)以前版本

■ iPad Pro(所有機型)、iPad Air 2、iPad 5(含)以上機型及 iPad mini 4(含)以上機型：iPadOS 14.8(不含)以前版本

(三) [建議措施:]

目前蘋果官方已針對此漏洞釋出更新程式，請各機關聯絡維護廠商或參考以下網址進行更新：

https://support.apple.com/en-us/HT201222

(四) [參考資料:]

1. https://support.apple.com/en-us/HT201222
2. https://www.ithome.com.tw/news/146698

二、【漏洞預警】微軟Windows作業系統存在多個安全漏洞，允許攻擊者取得權限或遠端執行任意程式碼，請儘速確認並進行更新。

(一) [內容說明:]

轉發 國家資安資訊分享與分析中心 資安訊息警訊 NISAC-ANA-202109-0847

研究人員發現 Windows 作業系統存在下列安全漏洞，遠端攻擊者可藉由漏洞取得權限或進而執行任意程式碼。

1.遠端執行任意程式碼漏洞：CVE-2021-36965 與 CVE-2021-38647。

2.權限提升漏洞：CVE-2021-36955、CVE-2021-36963、CVE-2021-36968、CVE-2021-38633、CVE-2021-38645、CVE-2021-38648、CVE-2021-38649、CVE-2021-38667、CVE-2021-38671 及 CVE-2021-40447。

情資分享等級: WHITE(情資內容為可公開揭露之資訊)

(二) [影響平台:]

1.CVE-2021-36955、CVE-2021-36963、CVE-2021-36965、CVE-2021-38633、CVE-2021-38667、CVE-2021-38671 及 CVE-2021-40447：

■ Windows 7 for 32-bit Systems Service Pack 1
■ Windows 7 for x64-based Systems Service Pack 1
■ Windows 8.1 for 32-bit systems
■ Windows 8.1 for x64-based systems
■ Windows RT 8.1 Windows 10 for 32-bit Systems
■ Windows 10 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems
■ Windows 10 Version 1607 for x64-based Systems
■ Windows 10 Version 1809 for 32-bit Systems
■ Windows 10 Version 1809 for ARM64-based Systems
■ Windows 10 Version 1809 for x64-based Systems
■ Windows 10 Version 1909 for 32-bit Systems
■ Windows 10 Version 1909 for ARM64-based Systems
■ Windows 10 Version 1909 for x64-based Systems
■ Windows 10 Version 2004 for 32-bit Systems
■ Windows 10 Version 2004 for ARM64-based Systems
■ Windows 10 Version 2004 for x64-based Systems
■ Windows 10 Version 20H2 for 32-bit Systems
■ Windows 10 Version 20H2 for ARM64-based Systems
■ Windows 10 Version 20H2 for x64-based Systems
■ Windows 10 Version 21H1 for 32-bit Systems
■ Windows 10 Version 21H1 for ARM64-based Systems
■ Windows 10 Version 21H1 for x64-based Systems
■ Windows Server 2008 for 32-bit Systems Service Pack 2
■ Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
■ Windows Server 2008 for x64-based Systems Service Pack 2
■ Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)

■ Windows Server 2008 R2 for x64-based Systems Service Pack 1
■ Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
■ Windows Server 2012
■ Windows Server 2012 (Server Core installation)
■ Windows Server 2012 R2
■ Windows Server 2012 R2 (Server Core installation)
■ Windows Server 2016
■ Windows Server 2016 (Server Core installation)
■ Windows Server 2019
■ Windows Server 2019 (Server Core installation)
■ Windows Server 2022
■ Windows Server 2022 (Server Core installation)
■ Windows Server, version 2004 (Server Core installation)
■ Windows Server, version 20H2 (Server Core Installation)

2.CVE-2021-38645、CVE-2021-38647、CVE-2021-38648 及 CVE-2021-38649：
Azure Open Management Infrastructure CVE-2021-36968：

■ Windows 7 for 32-bit Systems Service Pack 1
■ Windows 7 for x64-based Systems Service Pack 1
■ Windows Server 2008 R2 for x64-based Systems Service Pack 1
■ Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
■ Windows Server 2008 for 32-bit Systems Service Pack 2
■ Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
■ Windows Server 2008 for x64-based Systems Service Pack 2
■ Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)

(三) [建議措施:]
目前微軟官方已針對此漏洞釋出更新程式，請各機關聯絡維護廠商或參考以下網址進行更新：
1.https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36955
2.https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36963
3.https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36965
4.https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36968
5.https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38633
6.https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38645
7.https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38647
8.https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38648
9.https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38649
10.https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38667
11.https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38671
12.https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40447

（四）[參考資料:]

1. https://www.ithome.com.tw/news/146733
2. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36955
3. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36963
4. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36965
5. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36968
6. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38633
7. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38645
8. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38647
9. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38648
10. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38649
11. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38667
12. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38671
13. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40447

三、【漏洞預警】VMware vCenter存在多個安全漏洞(CVE-2021-21991~21993、22005~22020)，允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新。

(一) [內容說明:]

轉發 國家資安資訊分享與分析中心 資安訊息警訊 NISAC-ANA-202109-1275

研究人員發現 VMware vCenter 存在多個安全漏洞(CVE-2021-21991~21993、22005~22020)，遠端攻擊者可針對特定埠號利用漏洞上傳特製檔案，進而執行任意程式碼。

情資分享等級: WHITE(情資內容為可公開揭露之資訊)

(二) [影響平台:]

漏洞影響平台版本如下:

- vCenter Server 6.5 版本至 6.5 U3q 版本(不包含)
- vCenter Server 6.7 版本至 6.7 U3o 版本(不包含)
- vCenter Server 7.0 版本至 7.0 U2d 版本(不包含)
- Cloud Foundation (vCenter Server) 3.0 版本至 310.2.2 版本(不包含)
- Cloud Foundation (vCenter Server) 4.0 版本至 43.1 版本(不包含)

(三) [建議措施:]

VMware 官方已針對這些漏洞釋出更新程式，請各機關聯絡設備維護廠商或參考以下網址進行更新：

https://www.vmware.com/security/advisories/VMSA-2021-0020.html

(四) [參考資料:]

1. https://www.vmware.com/security/advisories/VMSA-2021-0020.html
2. https://thehackernews.com/2021/09/vmware-warns-of-critical-file-upload.html
3. https://www.ithome.com.tw/news/146841

四、**【漏洞預警】Google Chrome與Microsoft Edge瀏覽器存在安全漏洞(CVE-2021-37974~37976)，允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新。**

(一) [內容說明:]

轉發 國家資安資訊分享與分析中心 資安訊息警訊 NISAC-ANA-202110-0147

研究人員發現 Google Chrome 與 Microsoft Edge(基於 Chromium)瀏覽器存在安全漏洞(CVE-2021-37974~37976)，攻擊者可藉由誘騙受害者瀏覽特製網頁，利用此漏洞進而遠端執行任意程式碼。

情資分享等級: WHITE(情資內容為可公開揭露之資訊)

(二) [影響平台:]

- Google Chrome 94.0.4606.71 (不含)以前版本
- Microsoft Edge 94.0.992.38 (不含)以前版本

(三) [建議措施:]

1.請更新 Google Chrome 瀏覽器至 94.0.4606.71 以後版本，更新方式如下：

(1)開啟瀏覽器，於網址列輸入 chrome://settings/help，瀏覽器將執行版本檢查與自動更新

(2)點擊「重新啟動」完成更新

2.請更新 Microsoft Edge 瀏覽器至 94.0.992.38 以後版本，更新方式如下：

(1)開啟瀏覽器，於網址列輸入 edge://settings/help，瀏覽器將執行版本檢查與自動更新

(2)點擊「重新啟動」完成更新

(四) [參考資料:]

1. https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_30.html
2. https://www.ithome.com.tw/news/147017
3. https://thehackernews.com/2021/09/update-google-chrome-asap-to-patch-2.html
4. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37974
5. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37975
6. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37976

五、**【漏洞預警】SonicWall之SMA 100系列SSL VPN設備存在安全漏洞(CVE-2021-20034)，允許攻擊者繞過目錄遍歷檢查並刪除任意檔案，請儘速確認並進行更新。**

(一) [內容說明:]

轉發 國家資安資訊分享與分析中心 資安訊息警訊 NISAC-ANA-202109-1472

研究人員發現 SonicWall 之 SMA 100 系列 SSL VPN 設備存在安全漏洞(CVE-2021-20034)，肇因於存取控制失當，導致攻擊者可繞過目錄遍歷檢查並刪除任意檔案，進而造成設備重新啟動並還原至出廠設定。

情資分享等級: WHITE(情資內容為可公開揭露之資訊)

(二) [影響平台:]

SMA 100 系列(SMA 200、SMA 210、SMA 400、SMA 410 及 SMA 500v (ESX, KVM, AWS, Azure))之以下版本：

- 10.2.1.0-17sv(含)以前版本
- 10.2.0.7-34sv(含)以前版本
- 9.0.0.10-28sv(含)以前版本

(三) [建議措施:]

目前 SonicWall 官方已針對此漏洞釋出更新程式，請各機關聯絡設備維護廠商參考下方步驟進行版本更新：

https://www.sonicwall.com/support/product-notification/security-notice-critical-arbitrary-file-delete-vulnerability-in-sonicwall-sma-100-series-appliances/210819124854603/

(四) [參考資料:]

1. https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0021
2. https://thehackernews.com/2021/09/sonicwall-issues-patches-for-new.html
3. https://www.sonicwall.com/support/product-notification/security-notice-critical-arbitrary-file-delete-vulnerability-in-sonicwall-sma-100-series-appliances/210819124854603/

六、**【資安訊息】 NSA、CISA 分享 VPN 資訊安全小撇步以防禦駭客攻擊。**

(一) [內容說明:]

轉發 衛生福利部資安資訊分享與分析中心 資安訊息警訊 HISAC-ANA-202109-0005

美國網路安全和基礎設施安全局 (CISA) 和國家安全局 (NSA) 發布了加強虛擬專用網路 (VPN) 解決方案。案例分析:

1. 這兩個機構創建該文件是為了幫助組織提高防禦能力，特別是針對來自國家級駭客過去曾利用 VPN 系統中的漏洞竊取憑證、遠端執行代碼、減弱加密流量、劫持加密流量、並從設備中竊取敏感資料。

2. 作為加強 VPN 的準則，這兩個機構建議透過以下方式減少伺服器的攻擊面：

(1).在配置需增強加密和身份驗證。

(2).在嚴格必要的功能上運作。

(3).在受保護和監控下對 VPN 存取。

3. 今年 4 月初，網路安全公司 FireEye 發布了一份報告，在針對美國國防工業基地 (DIB) 的攻擊中使用了 Pulse Connect Secure (PCS) VPN 設備中的零時差漏洞。

4. 大約在同一時間，NSA 和 CISA 警告，為俄羅斯外國情報局 (SVR) 工作的駭客 APT29、Cozy Bear 和 The Dukes 已經成功利用 Fortinet 和 Pulse Secure VPN 設備中的漏洞進行攻擊。

5. 英國國家網路安全中心 (NCSC) 在 5 月發布一份諮詢報告，將思科和其他網路設備供應商的設備添加到俄羅斯外國情報局 (SVR) 工作的駭客所利用存在的漏洞產品列表中。

6. 勒索軟體集團也對這種類型的網路存取漏洞表現出極大的興趣，至少利用了 Fortinet、Ivanti (Pulse) 和 SonicWall 的 VPN 解決方案中的漏洞。

7. Cring、Ragnar Locker、Black Kingdom、 HelloKitty、LockBit、REvil、Conti 勒索軟體已成功透過利用 VPN 安全漏洞問題破壞了數十家公司。

情資分享等級: WHITE(情資內容為可公開揭露之資訊)

(二) [影響平台:]

無

(三) [建議措施:]

無

(四) [參考資料:]

https://www.bleepingcomputer.com/news/security/nsa-cisa-share-vpn-security-tips-to-defend-against-hackers-edited/

七、**【漏洞預警】Apache HTTP伺服器存在安全漏洞(CVE-2021-42013)，允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新。**

(一) [內容說明:]

轉發 國家資安資訊分享與分析中心 資安訊息警訊 NISAC-ANA-202110-0425

研究人員發現 Apache HTTP 伺服器存在安全漏洞(CVE-2021-42013)，攻擊者可藉由發送特製請求，利用此漏洞進而遠端執行任意程式碼。

情資分享等級: WHITE(情資內容為可公開揭露之資訊)

(二) [影響平台:]

● Apache HTTP Server 2.4.49 與 2.4.50 版本

(三) [建議措施:]

目前 Apache 官方已針對此漏洞釋出更新程式(更新版為 2.4.51)，請各機關儘速聯絡設備維護廠商或參考以下網址進行更新：

https://httpd.apache.org/security/vulnerabilities_24.html

(四) [參考資料:]

1. https://httpd.apache.org/security/vulnerabilities_24.html
2. https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-httpd-pathtrv-LAzg68cZ
3. https://www.openwall.com/lists/oss-security/2021/10/07/6