附件 3

111年3月8日～111年4月7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、Mozilla Firefox、Firefox ESR、Firefox for Android、Focus及Thunderbird等產品存在安全漏洞(CVE-2022-26485與CVE-2022-26486)，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 NISAC-ANA-202203-0389

研究人員發現Mozilla Firefox、Firefox ESR、Firefox for Android、Focus及Thunderbird等產品存在安全漏洞(CVE-2022-26485與CVE-2022-26486)，肇因於參數處理過程中移除XSLT參數，造成使用釋放後記憶體(Use-after-free)漏洞，或因參數檢查不足，導致WebGPU IPC框架存在沙箱逃逸(Sandbox escape)漏洞，結合上述兩個漏洞，將允許攻擊者遠端執行任意程式碼，且Mozilla表示已發現有攻擊程式利用漏洞發動攻擊。

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:]

- Firefox 97.0.2 以前版本
- Firefox ESR 91.6.1 以前版本
- Firefox for Android 97.3 以前版本
- Firefox Focus 97.3 以前版本
- Mozilla Thunderbird 91.6.2 以前版本

(三) [建議措施:]

Mozilla已修補漏洞並推出新版本，請更新各受影響產品至最新版本，更新方式如下：

1.Firefox與Firefox ESR版本檢查與更新方式如下：

(1)開啟瀏覽器，點擊選單按鈕，點選「說明」-->「關於Firefox」，可查看當前使用之Firefox瀏覽器是否為受影響之版本，瀏覽器將執行版本檢查與更新。

(2)點擊「重新啟動以更新Firefox」完成更新。

2.Firefox for Android版本檢查與更新方式如下：

(1)開啟瀏覽器，點擊選單按鈕，點選「設定」-->「關於Firefox」，版本號碼將會顯示在Firefox Browser文字標誌下方。

(2)可於裝置中之Google Play商店檢查是否有可用之更新，有可更新之版本時，將顯示於可更新列表上，點選「更新」完成更新。

3.Firefox Focus版本檢查與更新方式如下：

(1)開啟瀏覽器，點擊選單按鈕，點選「選項」-->「Mozilla」-->「關於Firefox Focus」。版本號碼將會顯示在Firefox Focus文字標誌下方。

(2)可於裝置中之Google Play商店檢查是否有可用之更新，有可更新之版本時，將顯示於可更新列表上，點選「更新」完成更新。

4.Thunderbird版本檢查與更新方式如下：

(1)開啟Thunderbird，點選「說明」-->「關於Mozilla Thunderbird」，可查看當前使用之Mozilla Thunderbird是否為受影響之版本，並執行版本檢查與更新。
(2)點擊「重新啟動以更新Thunderbird」完成更新。

5.保持良好使用習慣，請勿點擊來路不明的網址連結。

(四) [參考資料:]

1. https://www.ithome.com.tw/news/149738
2. https://www.mozilla.org/en-US/security/advisories/mfsa2022-09
3. https://support.mozilla.org/zh-TW/kb/update-latest-version-firefox-android
4. https://support.mozilla.org/en-US/kb/updating-thunderbird

二、**美國FBI發布RagnarLocker勒索軟體威脅指標，請各領域會員加強偵測與防護**

(一) [內容說明:]

轉發　國家資安資訊分享與分析中心 NISAC-ANA-202203-0504

因應RagnarLocker勒索軟體對能源、金融、政府及高科技等CI領域造成多起資安事件，美國FBI發布相關防護建議，技服中心綜整相關資料供各會員參考，內容詳見建議措施。

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:]

Windows平台

(三) [建議措施:]

1. 針對附件提供之威脅指標(indicators of compromise, IOCs)落實部署防護機制。

2. 加強電子郵件安全防護與惡意程式檢測。

3. 加強網路設備之威脅偵測與連線行為監控。

4. 為強化勒索軟體資安防護，建議強化下列安控措施：

(1) 部署多因子身分鑑別機制，並強化密碼管理。

(2) 落實資料、系統映像檔及組態設定之備份作業，且備份檔應離線保存並定期測試。

(3) 即時更新系統軟體版本與修補漏洞。

(4) 停用不必要之遠端服務與通訊埠，並落實監控遠端存取日誌。

(5) 定期稽核特權帳號與存取規則，落實最小存取權限原則。

5. 如有發現異常應立即進行通報。

附件-FBI 的 CU-000163-MW Flash Alert 警報：https://www.ic3.gov/Media/News/2022/220307.pdf

(四) [參考資料:]

https://www.cisa.gov/uscert/ncas/current-activity/2022/03/08/fbi-releases-indicators-compromise-ragnarlocker-ransomware

三、**請各單位加強網站安全檢查，並強化資安防護措施**

(一) [內容說明:]

近期國際政經情勢動盪，國家級網軍活動頻繁，除行政院國家資通安全會報技術服務中心已發布大規模攻擊活動預警，亦發現教育機構網站頁面遭駭客竄改狀況發生。

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:]

各單位相關資通系統與所屬網站等

(三) [建議措施:]

1.落實資通系統相關設備之安全性更新（包含作業系統、應用程式等）、安全性檢測（如弱點掃描、滲透測試、源碼掃描等）重大弱點之修補，確實實施資通系統防護基準。

2.依資安法相關規定，定期審查所保留資通系統產生之日誌(Log)，檢視有無異常登入、存取及操作行為。

3.請加強監控不尋常或未授權之活動（例如:網站被竄改、log有異常登入、存取及操作行為等）。

如屬資安事件，需依臺灣學術網路各級學校資通安全通報應變作業程序辦理。

(四) [參考資料:]

行政院國家資通安全會報技術服務中心 106年Web應用程式安全參考指引(修訂)v2.1_1101231.rar https://download.nccst.nat.gov.tw/attachfilecomm/106%E5%B9%B4Web%E6%87%89%E7%94%A8%E7%A8%8B%E5%BC%8F%E5%AE%89%E5%85%A8%E5%8F%83%E8%80%83%E6%8C%87%E5%BC%95(%E4%BF%AE%E8%A8%82)v2.1_1101231.rar

四、**請各單位對Sapido無線分享器進行漏洞檢測與修補作業，並強化資安防護措施。**

(一) [內容說明:]

由於Sapido(傻多)無線分享器存在CVE-2019-19822與CVE-2019-19823兩大漏洞，導致駭客透過漏洞可取得無線分享器之管理者帳號與密碼。在駭客入侵設備後會開啟VPN服務，並新增VPN帳戶 (VPN中繼站)。駭客也可在無需輸入帳密狀況下，直接遠端命令執行後門網頁，可以透過遠端登入http://(路由器ip)/syscmd.htm 或syscmd.asp，並以 Root 權限執行命令。

又該廠牌分享器之廠商久未更新韌體版本，加上分享器管理頁面可直接使用預設帳密(admin/admin)登入，顯示Sapido無線分享器存在很大資安問題。近期發現有多所學校使用Sapido無線分享器之情形，請使用該廠牌分享器之單位盡快檢視該設備之狀況，並且進行資安處理措施。

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:]

Sapido(傻多)無線分享器

(三) [建議措施:]

1.因廠商Sapido並未對相關漏洞進行修補，故建議停用該廠牌無線分享器。

2.建議勿使用預設之帳號與密碼登入設備之管理頁面，分享器上所有帳號需設定具強度之密碼，非必要使用之帳號請將其刪除或停用。

3.建議設備不要使用公開的網際網路位置，如無法避免使用公開之網際 網路位置，則建議設備前端需有防火牆防護並紀錄可疑異常連線。當發現惡意連線IP時，可加入防火牆黑名單進行阻擋。

4.因駭客通常透過外部網路連線功能入侵分享器，如非必要，可將相關功能關閉(例如:不允許從外部網路登入)。由於駭客使用分享器的方式多是透過 VPN 進行存取，建議可定期檢視分享器之VPN服務是否有開啟，並於防火牆觀察是否有大量異常的 VPN流量，可及早發現駭客的攻擊。

如屬資安事件，需依臺灣學術網路各級學校資通安全通報應變作業程序辦理。

(四) [參考資料:]

1. https://nvd.nist.gov/vuln/detail/CVE-2019-19822
2. https://nvd.nist.gov/vuln/detail/CVE-2019-19823

五、**Sophos UTM 高風險安全性漏洞**

(一) [內容說明:]

轉發 科學園區資安資訊分享與分析中心(SP-ISAC) SPISAC-ANA-202203-0010

Sophos UTM出現高風險安全性漏洞，此漏洞是由於Sophos UTM的郵件管理系統出現SQL injection，讓攻擊者可以繞過身份驗證並在Sophos UTM上執行任意代碼。

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:]

Sophos UTM v9.710 以前

(三) [建議措施:]

請更新至最新版本Sophos UTM v9.710 MR10

(四) [參考資料:]

https://www.sophos.com/en-us/security-advisories/sophos-sa-20220321-utm-9710

六、**Sophos Firewall作業系統存在安全漏洞(CVE-2022-1040)，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 NISAC-ANA-202203-0951

研究人員發現Sophos Firewall作業系統之使用者入口(User portal)與網頁管理介面(Webadmin)存在身分驗證繞過漏洞(CVE-2022-1040)，導致攻擊者得以利用該漏洞繞過系統管控，以管理者權限執行任意程式碼。

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:]

Sophos Firewall 18.5 MR3(含)以前版本

(三) [建議措施:]

1.目前Sophos官方已針對此漏洞釋出更新程式，請各機關可聯絡設備維護廠商進行版本更新，並確認更新至18.5 MR4(含)或19.0 GA以上版本。

2.如欲沿用舊版本，可登入網頁管理介面並啟用「允許自動安裝修補程式(Allow automatic installation of hotfixes)」功能，設備將每隔30分鐘檢查一次並自動安裝新修補程式，即可完成安裝此漏洞之修補程式。

3.若未能及時修補漏洞，可使用VPN或Sophos Central進行遠端連線與管理，以確保Sophos Firewall之網頁管理介面不暴露於廣域網路(WAN)中，以提升遠端存取安全性。

(四) [參考資料:]

1. https://www.sophos.com/en-us/security-advisories/sophos-sa-20220325-sfos-rce
2. https://nvd.nist.gov/vuln/detail/CVE-2022-1040
3. https://www.bleepingcomputer.com/news/security/critical-sophos-firewall-vulnerability-allows-remote-code-execution/

七、SonicWall SonicOS存在安全漏洞(CVE-2022-22274)，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 NISAC-ANA-202204-0007

SonicOS 是 SonicWall 防火牆所使用之作業系統，研究人員發現 SonicOS 存在堆疊記憶體緩衝溢位(Stack-based buffer overflow)漏洞，遠端攻擊者可藉由發送特製之 HTTP 請求，利用此漏洞進行阻斷服務攻擊或執行任意程式碼。

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.SonicWall FireWalls

(1)型號：TZ270, TZ270W, TZ370, TZ370W, TZ470, TZ470W, TZ570, TZ570W, TZ570P, TZ670, NSa 2700, NSa 3700, NSa 4700, NSa 5700, NSa 6700, NSsp 10700, NSsp 11700, NSsp 13700, NSv 270, NSv 470, NSv 870

(2)SonicOS 版本：7.0.1-5050(含)以前版本

2.SonicWall NSsp Firewall

(1)型號：NSsp 15700

(2)SonicOS 版本：7.0.1-R579(含)以前版本

3.SonicWall NSv Firewalls

(1)型號：NSv 10, NSv 25, NSv 50, Nsv 100, NSv 200, NSv 300, NSv 400, NSv 800, NSv 1600

(2)SonicOS 版本：6.5.4.4-44v-21-1452(含)以前版本

(三) [建議措施:]

1.目前 SonicWall 官方已針對此漏洞釋出部份更新程式，請各機關可聯絡設備維護廠商進行下列版本更新作業：

(1)SonicWall FireWalls：請更新至 7.0.1-5051(含)以上版本。

(2)SonicWall NSsp Firewall：請採取緩解措施，僅允許受信任之來源 IP 可連線至管理介面，或安裝 7.0.1-5030-HF-R844 修補程式。俟 SonicWall 官方 4 月中釋出新版程式後，再進行 SonicOS 升版作業。

(3)SonicWall NSv Firewalls：請更新至 6.5.4.4-44v-21-1519(含)以上版本。

2.設備管理者登入管理介面後，可於監控功能頁面之系統狀態資訊中，得知該設備所使用之 SonicOS 版本。

(四) [參考資料:]

1. https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003
2. https://nvd.nist.gov/vuln/detail/CVE-2022-22274
3. https://www.bleepingcomputer.com/news/security/critical-sonicwall-firewall-patch-not-released-for-all-devices/

八、Google Chrome、Microsoft Edge、Brave、Vivaldi及Opera瀏覽器存在高風險安全漏洞(CVE-2022-1096)，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 NISAC-ANA-202203-1099

研究人員發現 Google Chrome、Microsoft Edge、Brave、Vivaldi 及 Opera 等以 Chromium 為基礎之瀏覽器，皆存在 Chrome V8 JavaScript 引擎之類型混淆(Type Confusion)漏洞(CVE-2022-1096)，攻擊者可利用此漏洞造成瀏覽器當機或緩衝區溢位，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 99.0.4844.84(不含)以前版本
- Microsoft Edge 99.0.1150.55(不含)以前版本
- Brave 1.36.122(不含)以前版本
- Vivaldi 5.1.2567.73 (不含)以前版本
- Opera 85.0.4341.28(不含)以前版本

(三) [建議措施:]

1.請更新 Google Chrome 瀏覽器至 99.0.4844.84 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 99.0.1150.55 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

3.請更新 Brave 瀏覽器至 1.36.122 以後版本，更新方式如下：

(1)開啟瀏覽器，於網址列輸入 brave://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

4.請更新 Vivaldi 瀏覽器至 5.1.2567.73 以後版本，更新方式如下：

(1)開啟瀏覽器，點選左上方 Vivaldi 圖示開啟下拉式選單，點選 說明>檢查更新

(2)點擊「重新啟動」完成更新

5.請更新 Opera 瀏覽器至 85.0.4341.28 以後版本，更新方式如下：

(1)開啟瀏覽器，於網址列輸入 opera://settings/about，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://www.informationsecurity.com.tw/article/article_detail.aspx?aid=9785
2. https://www.ithome.com.tw/news/150121
3. https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop_25.html
4. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1096
5. https://github.com/brave/brave-browser/issues/21889
6. https://vivaldi.com/blog/desktop/minor-update-five-5-1/
7. https://blogs.opera.com/desktop/changelog-for-85/

九、**請各單位建立網站公告內容審查機制，以避免未經授權可直接取得個人資料外洩。**

(一) [內容說明:]

鑑於近日發生學校網站未適當處理公告內容，造成個人資料(以下簡稱個資)外洩，以嚴重影響當事人權利。重申各單位應建立並落實網站公告內容之審查機制，加強控管，以避免個資外洩發生。

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:]

學校相關網站

(三) [建議措施:]

1.請各單位儘速檢視單位網站公告內容，是否存在未經授權可直接個資(例如:姓名、出生年月日、聯絡方式或其他得以直接或間接方式識別個資) 如有者，請儘速下架，並移除暫存網頁之資料 (例如:申請 Google 搜尋中移除個人資料)。

2.定期檢視存放於單位網站上之公開資訊及公告附件檔案，是否含有未經授權可直接取得個資。建議使用搜尋引擎查詢單位網站公告內容，相關查詢語法可參考「臺灣學術網路個資外洩事件之預防與應變指南」，並檢視是否有含有未經授權之個資檔案放置網站上。

3.請各單位建立並落實公告於單位網站內容之審查機制(例如:單位主管審核流程)。若有需要公告相關個資請進行遮罩方式處理，以避免造成個資外洩風險。

4.以上請各單位配合並積極落實，若發生個資外洩將依相關規定進行處置。

(四) [參考資料:]

1、臺灣學術網路個資外洩事件之預防與應變指南
https://portal.cert.tanet.edu.tw/docs/pdf/202106250406151547456138838637 4.pdf
2.個人資料保護法 https://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050021
3.申請Google搜尋中移除個人資料 https://support.google.com/websearch/answer/9673730

十、請各單位全面盤點含有個人資料之系統，並遵守資通系統防護基準規範。

(一) [內容說明:]

為防範各單位於系統開發與維護過程產生疏漏，導致個資外洩之資安事件發生，籲請各校積極落實系統開發之維護管理作業，並應遵守安全軟體開發生命週期(SSDLC)與符合資通系統防護基準規範。

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:]

N/A

(三) [建議措施:]

1.應全面性盤點含有個人資料之系統，檢視儲存個人資料之適法性與必要性，並納入資訊安全管理制度(ISMS)。

2.應落實核心系統資產盤點、帳號清查及定期進行備份作業，如有變更需即時更新 ISMS 相關文件。

3.在進行系統開發與維護時須遵守「資通安全責任等級分級辦法」之「附表十資通系統防護基準」規範，提供適當之資安防護措施。

4.在系統發展生命週期之「開發階段」應執行「源碼掃描」安全檢測。針對安全需求實作必要控制措施。應注意避免軟體常見漏洞及實作必要控制措施。發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。

5.在系統發展生命週期之「測試階段」應執行「弱點掃描」與「滲透測試」安全檢測，並於系統上線前完成弱點修補。在確認無中、高風險弱點後方可上線。

6.在系統發展生命週期之「部署與維運階段」應執行版本控制與變更管理。於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。所開發資通系統不使用預設密碼。

7.在維護系統時如需更新系統版本，應確認所更新程式是否為正確上架版本，避免因上架錯誤版本造成機敏資料外洩風險。建議採用雙人複核機制，確認版本無誤後再進行上架作業。

8.在系統發展生命週期之「委外階段」若資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求（含機密性、可用性、完整性）納入委外契約。

9.各單位之資通系統應每年度進行滲透測試，檢測項目應包含系統弱點分析、網站弱點分析、OWASP Top 10 檢測、人工邏輯檢測等作業，並且應強化人工邏輯檢測作業項目。滲透測試需經初、複掃雙重驗證方式來確認弱點修補品質，並透過專家指導快速排除已知之風險與問題。

(四) [參考資料:]

1.「資通安全責任等級分級辦法」之附表十資通系統防護基準.pdf https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030304