行政院國家資通安全會報技術服務中心

近兩年駭客最常利用之29個漏洞資訊與修補方式

發布日	110/8/9

1. 概述

美國網路安全暨基礎架構管理署(Cybersecurity and Infrastructure Security Agency , CISA)、美國聯邦調查局(Federal Bureau of Investigation, FBI)、澳州網路安全中心(Australian Cyber Security Centre, ACSC)及英國國家網路安全中心(National Cyber Security Centre, NCSC)於7月28日共同發布資安公告，彙整2020年迄今駭客最常利用之29個漏洞資訊與修補方式，呼籲各政府機關(構)與企業儘速修補這些漏洞。

2. 漏洞說明與修補方式

2020年迄今駭客最常利用之29個漏洞綜整如下表，受影響廠商計有11家，其中以Microsoft有9個漏洞為最多。2020年前4大漏洞分別是Citrix (CVE-2019-19781)、Fortinet (CVE-2018-13379)、Pulse Secure (CVE-2019-11510)及F5 (CVE 2020-5902)，皆為VPN漏洞，2021年常遭駭客利用之漏洞則包含Microsoft Exchange Server漏洞(包含CVE-2021-26855、26857、26858及27065)、美國Accellion檔案分享服務漏洞(CVE-2021-27101~27104)及VMWare vCenter漏洞(CVE-2021-2198)，且結合多個漏洞進行串連攻擊為近期常見之攻擊手法。

項次	廠商	CVE編號
1	Accellion	CVE-2021-27101~27104
2	Atlassian	CVE-2019-3396、CVE-2019-11580
3	Citrix	CVE-2019-19781

4	Drupal	CVE-2018-7600
5	F5	CVE-2020-5902
6	Fortinet	CVE 2018-13379、CVE-2019-5591、CVE-2020-12812
7	Microsoft	CVE-2017-11882、CVE-2019-0604、CVE-2020-0688、CVE-2020-0787、CVE-2020-1472、CVE-2021-26855、CVE-2021-26857、CVE-2021-26858、CVE-2021-27065
8	MobileIron	CVE 2020-15505
9	Pulse Secure	CVE-2019-11510、CVE-2021-22893、CVE-2021-22894、CVE-2021-22899、CVE-2021-22900
10	Telerik	CVE-2019-18935
11	VMware	CVE-2021-21985

個別漏洞之技術細節與修補方式依 CVE 編號順序說明如下：

2.1.CVE-2017-11882

Microsoft Office 存在記憶體毀損漏洞，因 Office 未正確處理記憶體中的物件，導致攻擊者僅需在文件中嵌入特定程式碼，透過社交工程等方式誘騙使用者開啟，進而可遠端執行任意程式碼。

2.1.1. 技術細節

- Microsoft 程式編輯器(eqnedt32.exe)是 Microsoft Office 中的一個工具，可在文件中插入或編輯 OLE 物件，自 2000 年 11 月 9 日釋出後未再發布新版本，且支援當時所有 Microsoft Office 版本。該工具存在一個堆疊緩衝區溢位漏洞，造成可在系統上遠端執行任意程式碼。
- 資料執行防止(Data execution prevention, DEP)與位址空間組態隨機載入(Address Space Layout Randomization, ASLR)應能夠防止這類攻擊，但由於

eqnedt32.exe 的執行並未引入 ASLR 與 DEP 之防護，使得攻擊者仍可透過誘騙使用者開啟特製檔案，觸發所嵌入之攻擊指令後，進而可遠端執行任意程式碼。

2.1.2. 防護建議

●請至 Microsoft 官網下載並安裝修補程式，參考網址：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882。

●無法更新之用戶應禁用方程式編輯器，參考網址：https://support.microsoft.com/en-us/topic/how-to-disable-equation-editor-3-0-7e000f58-cbf4-e805-b4b1-fde0243c9a92。

2.2.CVE-2018-7600

Drupal 因預設與通用模組配置存在安全漏洞，允許攻擊者遠程執行任意程式碼。

2.2.1. 技術細節

Drupal 7.x 與 8.x 版本因未嚴格過濾表單請求，導致遠端攻擊者可藉由瀏覽 Drupal 網站上特定 URL 並發送特定惡意表單請求，進而可遠端執行任意程式碼，若攻擊失敗亦可導致網站服務中斷。

2.2.2. 防護建議

請參考 Drupal 官網公告(https://www.drupal.org/sa-core-2018-002)，依所使用版本進行下列更新作業：

●Drupal 7.x 版本請更新至 Drupal 7.58 以上版本。

●Drupal 8.5.x 版本請更新至 Drupal 8.5.1 以上版本。

2.3.CVE-2018-13379

Fortinet Secure Sockets Layer (SSL) VPN 存在一個無需身分驗證之目錄遍歷(Path traversal)漏洞，攻擊者可在未獲授權之情況下，透過此漏洞存取 sslvpn_websession 檔案，進而取得明文用戶帳號與密碼。

2.3.1. 技術細節

用戶存取控制與 Web 應用程式目錄結構存在漏洞，允許攻擊者在未經身分驗證之情況下，藉由執行「HTTP GET request http://$SSLVPNTARGET?lang=/../../../..//////////dev/cmdb/sslvpn_websession」指令，成功存取 sslvpn_websession 檔案，進而取得可登入 VPN 之明文帳號與密碼。

2.3.2. 防護建議

- 請至 Fortinet 官網下載並安裝更新軟體版本，參考網址：https://www.fortiguard.com/psirt/FG-IR-18-384。
- 監控任何排程任務外或未知/可執行文件之提醒警告。
- 建立偵測與保護機制，當嘗試透過目錄遍歷方式讀取 sslvpn_websessions 檔案時予以告警。

2.4.CVE-2019-0604

Microsoft SharePoint 之 XML 反序列化套件存在漏洞，允許遠端攻擊者可在 SharePoint 伺服器上執行任意程式碼。

2.4.1. 技術細節

- 攻擊者可藉由此漏洞上傳惡意 webshell 至受影響之 IIS 網頁伺服器，並且不需身分驗證，惡意 webshell 通常上傳於 SharePoint 安裝目錄之 Layouts

資料夾中。

– C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\<version_number>\Template\Layouts

●XmlSerializer.Deserialize()函式未正確處理 picker.aspx PickerEnitity/ValidateEnity()函式中序列化 XML payload，當序列化 XML payload 被反序列化，就會執行相關程式碼。攻擊者可對基於.Net 之 XML 解析器上傳 XMLNS payload，於 payload 中帶入< system:string>標籤與惡意作業系統指令。

2.4.2. 防護建議

●請至 Microsoft 官網下載並安裝修補程式，參考網址：https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2019-0604。

●由外部網際網路連線之使用者應僅允許透過 VPN 連線至 SharePoint 伺服器。

2.5.CVE-2019-3396

Atlassian Confluence Server 與 Confluence Data Center 內之 Widget Connector 存在伺服器端模板注入(Server-side template injection)漏洞。

2.5.1. 技術細節

遠端攻擊者可利用 Widget Connector 之伺服器端模板注入漏洞，對 Confluence Server 與 Confluence Data Center 發送任意 HTTP 與 WebDAV 請求，利用此漏洞在未授權情況下進而遠端執行任意程式碼。

2.5.2. 防護建議

請至 Atlassian 官網下載並更新軟體版本，參考網址：https://confluence.atlassian.com/doc/confluence-security-advisory-2019-03-20-966660264.html。

2.6.CVE-2019-5591

FortiOS 預設設定存在漏洞，導致攻擊者可獲取機敏資料。

2.6.1. 技術細節

FortiOS 預設設定未驗證 LDAP 伺服器身分，導致位於同網段之攻擊者可藉由假冒 LDAP 伺服器，從中攔截獲取機敏資料。

2.6.2. 防護建議

請至 Fortinet 官網下載並更新軟體版本，參考網址：https://www.fortiguard.com/psirt/FG-IR-19-037。

2.7.CVE-2019-11510

Pulse Secure Connect SSL VPN 存在一個無需身分驗證之目錄遍歷(Path traversal)漏洞，攻擊者可利用此漏洞存取管理員登入資訊。

2.7.1. 技術細節

- 攻擊者可利用目錄遍歷漏洞讀取系統文件內容，例如攻擊者透過存取「https://sslvpn.insecure-org.com/dana-na/../dana/html5/acc/guacmole/../../../../../../etc/passwd?/dana/html5/guacamole/」網址，可成功從系統中取得密碼資訊，攻擊者透過所取得之資訊進而取得 VPN 管理權限。

2.7.2. 防護建議

- 請至 PulseSecure 官網下載並更新軟體版本，參考網址：

https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101。

●監控任何排程任務外或未知/可執行文件之提醒警告。

●建立偵測與保護機制，當嘗試透過目錄遍歷方式讀取本地系統文件時予以告警。

2.8.CVE-2019-11580

Atlassian 之 Crowd 與 Crowd Data Center 在釋出版本時誤啟用 pdkinstall 開發套件，導致攻擊者可遠端執行任意程式碼。

2.8.1. 技術細節

攻擊者藉由向 Atlassian Crowd 與 Crowd Data Center 發送惡意請求時，可利用此漏洞安裝任意惡意套件，進而在 Crowd 與 Crowd Data Center 系統上遠端執行任意程式碼。

2.8.2. 防護建議

請參考 Atlassian 官網公告(https://jira.atlassian.com/browse/CWD-5388)，依所使用版本進行下列更新作業：

●Crowd and Crowd Data Center 3.3.0(不含)以前版本請更新至 3.2.8 版本。

●Crowd and Crowd Data Center 3.3.x 版本請更新至 3.3.5 版本。

●Crowd and Crowd Data Center 3.4.x 版本請更新至 3.4.4 版本。

2.9.CVE-2019-18935

Telerik UI for ASP.NET AJAX 因未正確過濾序列化輸入內容，導致 Web 伺服器存在反序列化漏洞，進而導致遠程執行任意程式碼。

2.9.1. 技術細節

Telerik UI 存在反序列化漏洞，該漏洞發生在 HTTP POST 參數 rauPostData 中使用之 AsyncUploadHandler 函式，此函式所引用之 JavaScriptSerializer.Deserialize()函式在反序列化過程中未正確處理序列化資料，已知加密金鑰之遠端攻擊者可利用此漏洞執行任意程式碼。

2.9.2. 防護建議

請參考 Telerik 官網公告，更新 Telerik UI for ASP.NET AJAX 版本至 2020.1.114，參考網址：https://www.telerik.com/support/kb/aspnet-ajax/details/allows-javascriptserializer-deserialization。

2.10.CVE-2019-19781

Citrix Application Delivery Controller (ADC)由於存取控制不當，導致攻擊者利用目錄遍歷漏洞，進而遠端執行任意程式碼。

2.10.1. 技術細節

- 攻擊者利用不當的存取控管及目錄遍歷漏洞瀏覽 Citrix ADC (newbm.pl)，透過 HTTP POST 請求(POST https://$TARGET/vpn/../vpn/portal/scripts/newbm.pl)存取該腳本時，即可執行本地作業系統指令。
- 攻擊者利用上述漏洞可上傳與執行惡意程式，進而遠端執行任意程式碼。

2.10.2. 防護建議

請參考 Citrix 官網公告，依所使用版本進行更新作業，參考網址：https://support.citrix.com/article/CTX267679。

2.11.CVE-2020-0688

Microsoft Exchange 軟體未正確處理記憶體中物件，導致攻擊者可遠端執行

任意程式碼。

2.11.1. 技術細節

- 此漏洞肇因於 Exchange 伺服器未在安裝時建立唯一金鑰，使得攻擊者可透過授權使用者取得金鑰，利用傳遞特製 payload 到 Exchange 伺服器，造成記憶體毀損展開攻擊。
- 攻擊者需先透過授權使用者資訊，以開發者工具取得 ViewStateUserKey 與__VIEWSTATEGENERATOR 值後，利用公開的.NET 參數反序列化工具造訪特定頁面，便可遠端執行任意程式碼

2.11.2. 防護建議

請至 Microsoft 官網下載並安裝修補程式，參考網址：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-0688。

2.12.CVE-2020-0787

Windows 背景智慧型傳輸服務(BITS)因未正確處理符號連結，攻擊者可利用此漏洞提升權限。

2.12.1. 技術細節

當 Windows BITS 服務未正確處理符號連結時，存在一個提升權限漏洞。攻擊者首先使用低權限帳號登入系統，接著提供一個資料夾路徑(如 C:\Users\<username>\AppData\Local\Temp\workspace)給 BITS 服務，做為實體目錄之連結點，當符號連結執行移動操作時，因未正確處理符號連結，導致攻擊者可藉由覆寫任意目標檔案進行提權，進而完全控制所登入之系統。

2.12.2. 防護建議

請至 Microsoft 官網下載並安裝修補程式，參考網址：

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-0787。

2.13.CVE-2020-1472

Windows Netlogon 遠端協定(MS-NRPC)存在安全漏洞，允許攻擊者在未授權之狀況下提權至網域管理者權限。

2.13.1. 技術細節

使用 Netlogon 遠端協定(MS-NRPC)建立與網域控制站(Domain Controller)之安全通道時，存在可提升權限之安全漏洞，攻擊者在無任何網域登入帳密之狀況下，僅需針對存在漏洞之網域控制站(DC)建立安全通道連線，即可利用此漏洞變更網域管理員密碼並取得網域管理者權限，進而在該網域中之電腦執行任意程式碼。

2.13.2. 防護建議

請至 Microsoft 官網下載並安裝修補程式，參考網址：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-1472。

2.14.CVE-2020-5902

F5 BIG-IP 產品存在安全漏洞，允許攻擊者遠端執行任意程式碼。

2.14.1. 技術細節

F5 BIG-IP 產品之流量管理用戶介面(Traffic Management User Interface，簡稱 TMUI)存在安全漏洞，遠端攻擊者可對目標設備發送特製請求，利用此漏洞進而遠端執行系統指令、寫入與刪除檔案、關閉服務及執行任意 Java 程式碼。

2.14.2. 防護建議

請至 F5 官網下載並更新軟體版本，若無法立即更新，可採取緩解措施(如限

制存取來源)降低風險，參考網址：
https://support.f5.com/csp/article/K52145254。

2.15.CVE-2020-12812

FortiOS SSL VPN 2FA 透過修改用戶名大小寫，可成功繞過雙因素身分驗證機制。

2.15.1. 技術細節

FortiOS 之 SSL VPN 身分驗證存在漏洞，當「user local」設定啟用雙因素身分驗證，且該用戶之身分驗證類型設為遠端驗證方式(如 ldap)時，因本地與遠端身分驗證之間的大小寫匹配不一致，導致攻擊者更改使用者名稱大小寫後，系統不會提示第二個身分驗證因素(FortiToken)，即可繞過雙因素身分驗證機制成功登入。

2.15.2. 防護建議

請至 Fortinet 官網下載並更新軟體版本，參考網址：
https://www.fortiguard.com/psirt/FG-IR-19-283。

2.16.CVE-2020-15505

MobileIron 移動設備管理(MDM)軟體伺服器存在漏洞，導致攻擊者可遠端執行任意程式碼。

2.16.1. 技術細節

MobileIron 旗下 Core & Connector、Sentry 及 Monitoring and Reporting Database(RDB)軟體存在漏洞，攻擊者可利用特製 HTTP 封包觸發漏洞，進而遠端執行任意程式碼。

2.16.2. 防護建議

請至 MobileIron 官網下載並安裝更新軟體版本，參考網址：https://www.ivanti.com/blog/mobileiron-security-updates-available?miredirect。

2.17.CVE-2021-21985

VMware vCenter 存在安全漏洞，允許攻擊者遠端執行任意程式碼

2.17.1. 技術細節

vCenter 伺服器中預設開啟之 vSAN plugin(Virtual SAN Health Check plugin)未完整驗證用戶提交的資料，導致遠端攻擊者可使用 vSphere 客戶端軟體(HTML5)藉由埠號 443 對 vCenter 伺服器發送特定格式封包，利用此漏洞進而執行任意程式碼。

2.17.2. 防護建議

請至 VMware 官網下載並更新軟體版本，若無法立即更新，可採取緩解措施(如限制存取來源)降低風險，參考網址：https://www.vmware.com/security/advisories/VMSA-2021-0010.html。

2.18.CVE-2021-22893

Pulse Secure 之 Pulse Connect Secure 產品存在漏洞，允許攻擊者遠端執行任意程式碼。

2.18.1. 技術細節

Pulse Connect Secure 9.1R11.4 以前版本存在漏洞，遠端攻擊者可藉由向目標設備發送特定 HTTP 請求封包，利用此漏洞繞過身分驗證機制取得管理員權限，進而執行任意程式碼。

2.18.2. 防護建議

請至 Pulse Secure 官網下載並更新軟體版本，參考網址：

https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44784。

2.19.CVE-2021-22894

Pulse Secure 之 Pulse Connect Secure Collaboration Suite 產品存在緩衝區溢位漏洞，導致攻擊者可遠端執行任意程式碼。

2.19.1. 技術細節

Pulse Connect Secure Collaboration Suite 9.1R11.4 以前版本存在緩衝區溢位漏洞，遠端合法使用者可藉由特製惡意的會議室，利用此漏洞以 root 身分執行任意程式碼。

2.19.2. 防護建議

請至 Pulse Secure 官網下載並更新軟體版本，參考網址：
https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44784。

2.20.CVE-2021-22899

Pulse Secure 之 Pulse Connect Secure 產品存在命令注入漏洞，導致攻擊者可遠端執行任意程式碼。

2.20.1. 技術細節

Pulse Connect Secure 9.1R11.4 以前版本存在命令注入漏洞，允許合法使用者透過 Windows 檔案資源配置文件執行任意程式碼。

2.20.2. 防護建議

請至 Pulse Secure 官網下載並更新軟體版本，參考網址：
https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44784。

2.21.CVE-2021-22900

Pulse Secure 之 Pulse Connect Secure 產品存在任意上傳檔案漏洞，攻擊者可以透過網頁任意上傳惡意檔案。

2.21.1. 技術細節

Pulse Secure Connect 9.1R11.4 之前版本存在任意上傳檔案漏洞，擁有管理者權限之帳號，可透過管理頁面任意上傳惡意檔案。

2.21.2. 防護建議

請至 Pulse Secure 官網下載並更新軟體版本，參考網址：https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44784。

2.22.CVE-2021-26855

Microsoft Exchange Server 存在伺服器請求偽造(Server Side Request Forgery，SSRF)漏洞，允許攻擊者遠端執行任意程式碼。

2.22.1. 技術細節

Microsoft Exchange SSRF 漏洞發生點位於 C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\bin 檔案目錄下的動態連結函式庫 Microsoft.Exchange.FrontEndHttpProxy.dll 中，因對 X-BEResource 欄位字串處理不當，使得攻擊者可在未經授權情況下，透過傳送特定封包以取得合法的 SID，進而取得有效 Cookie 繞過身分驗證機制取得管理者權限。

2.22.2. 防護建議

請至 Microsoft 官網下載並安裝修補程式，參考網址：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855。

2.23.CVE-2021-26857

Microsoft Exchange Server 存在不安全的反序列化漏洞，允許攻擊者遠端執行任意程式碼。

2.23.1. 技術細節

Microsoft Exchange Server 之 Unified Messaging 服務存在反序列化漏洞，攻擊者可在 Exchange Server 上利用此漏洞，進而以系統權限執行程式碼。

2.23.2. 防護建議

請至 Microsoft 官網下載並安裝修補程式，或關閉 Unified Messaging 服務，參考網址：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26857。

2.24.CVE-2021-26858

Microsoft Exchange Server 存在漏洞，允許攻擊者任意寫入檔案。

2.24.1. 技術細節

因 OAB(offline address book)設定不當，導致攻擊者可利用此漏洞任意寫入檔案。此漏洞可結合 CVE-2021-26855 進行漏洞串連攻擊，當繞過身分驗證機制後，攻擊者可利用此漏洞上傳惡意程式到任何位置，以進行後續攻擊與內部橫向移動。

2.24.2. 防護建議

請至 Microsoft 官網下載並安裝修補程式，參考網址：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26858。

2.25.CVE-2021-27065

Microsoft Exchange Server 存在漏洞，允許攻擊者任意寫入檔案。

2.25.1. 技術細節

Exchange ECP(Exchange Control Panel)管理介面中，虛擬目錄設定頁面之外部 URL 欄位未限制可輸入之內容，使得攻擊者可上傳.aspx 之惡意程式，透過存取該 aspx 檔案，Exchange 伺服器將以 aspx 格式進行解析，進而成功觸發與執行惡意程式。

2.25.2. 防護建議

請至 Microsoft 官網下載並安裝修補程式，參考網址：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-27065。

2.26.CVE-2021-27101

Accellion 旗下 File Transfer Appliance (FTA)產品存在 SQL 注入漏洞。

2.26.1. 技術細節

Accellion 旗下 FTA 9_12_370 之前版本因未正確過濾字元，攻擊者可在 document_root.html 頁面透過傳送特製的 HOST header 執行注入攻擊。

2.26.2. 防護建議

請更新 Accellion FTA 至 FTA_9_12_380 以上版本，參考網址：https://www.accellion.com/company/press-releases/accellion-responds-to-recent-fta-security-incident/。

●Accellion 宣布 FTA 產品於 2021 年 4 月 30 日終止支援，建議改採其他替代方案。

2.27.CVE-2021-27102

Accellion 旗下 File Transfer Appliance (FTA)產品存在系統指令注入漏洞。

2.27.1. 技術細節

Accellion 旗下 FTA 9_12_411 之前版本存在系統指令注入漏洞，攻擊者可透過本地端網頁服務執行注入攻擊。

2.27.2. 防護建議

- 請更新 Accellion FTA 至 FTA_9_12_416 以上版本，參考網址：https://www.accellion.com/company/press-releases/accellion-responds-to-recent-fta-security-incident/。
- Accellion 宣布 FTA 產品於 2021 年 4 月 30 日終止支援，建議改採其他替代方案。

2.28.CVE-2021-27103

Accellion 旗下 File Transfer Appliance (FTA)產品存在伺服器端請求偽造(Server-Side Request Forgery, SSRF)漏洞。

2.28.1. 技術細節

Accellion 旗下 FTA 9_12_411 之前版本存在伺服器端請求偽造漏洞，攻擊者可藉由傳送特製的 POST 請求封包至 wmProgressstat.html 頁面進行攻擊。

2.28.2. 防護建議

- 請更新 Accellion FTA 至 FTA_9_12_416 以上版本，參考網址：https://www.accellion.com/company/press-releases/accellion-responds-to-recent-fta-security-incident/。

●Accellion 宣布 FTA 產品於 2021 年 4 月 30 日終止支援，建議改採其他替代方案。

2.29.CVE-2021-27104

Accellion 旗下 File Transfer Appliance (FTA)產品存在系統指令注入漏洞。

2.29.1. 技術細節

Accellion 旗下 FTA 9_12_370 之前版本存在系統指令注入漏洞，攻擊者可透過傳送特製的 POST 封包對不同端點設備進行攻擊。

2.29.2. 防護建議

●請更新 Accellion FTA 至 FTA_9_12_380 以上版本，參考網址：https://www.accellion.com/company/press-releases/accellion-responds-to-recent-fta-security-incident/。

●Accellion 宣布 FTA 產品於 2021 年 4 月 30 日終止支援，建議改採其他替代方案。

3. 綜合建議措施

(1) 清查機關是否有使用受上述漏洞影響之軟體與設備，並及時完成漏洞修補

(2) 檢視主機對外開放的必要性，無特殊需求建議關閉不必要之通訊埠(如 137, 138, 139, 445, 3389 等)，僅開放必要服務。

(3) 確認作業系統、防毒軟體及應用程式(如 Adobe Flash Player、Java)更新情況，並定期檢視系統/應用程式更新紀錄，避免駭客利用系統/應用程式安全性漏洞進行入侵行為。

(4) 定期備份系統資料，並參考以下建議措施：

- 應確保備份資料無感染之虞，例如採用離線備份存放。
- 定期測試備份資料可有效還原。
- 針對機敏資料應進行存取控制管控與加密。

(5) 即時監測未授權之存取行為，透過專職監控人員或自動化機制偵測未經授權之存取行為，加強對伺服器、網路設備及個人電腦等設備之日誌監控。

(6) 加強資安教育訓練，使用者留意相關電子郵件，注意郵件之來源的正確性，不要開啟不明來源信件的附檔或連結。

(7) 建立良好的網段管理，確保隔離的網段可以獨自運行。

(8) 利用第三方滲透測試，確認系統安全性與抵禦攻擊的能力。

4. 參考資料

[1]https://us-cert.cisa.gov/ncas/alerts/aa21-209a

[2]https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882

[3]https://support.microsoft.com/en-us/topic/how-to-disable-equation-editor-3-0-7e000f58-cbf4-e805-b4b1-fde0243c9a92

[4]https://www.drupal.org/sa-core-2018-002

[5]https://www.fortiguard.com/psirt/FG-IR-18-384

[6]https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2019-0604

[7]https://confluence.atlassian.com/doc/confluence-security-advisory-2019-03-20-966660264.html

[8]https://www.fortiguard.com/psirt/FG-IR-19-037

[9]https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101

[10]https://jira.atlassian.com/browse/CWD-5388

[11]https://www.telerik.com/support/kb/aspnet-ajax/details/allows-javascriptserializer-deserialization

[12]https://support.citrix.com/article/CTX267679

[13]https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-0688

[14]https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-0787

[15]https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-1472

[16]https://support.f5.com/csp/article/K52145254

[17]https://www.fortiguard.com/psirt/FG-IR-19-283

[18]https://www.ivanti.com/blog/mobileiron-security-updates-available?miredirect

[19]https://www.vmware.com/security/advisories/VMSA-2021-0010.html

[20]https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44784

[21]https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855

[22]https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26857

[23]https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26858

[24]https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-27065

[25]https://www.accellion.com/company/press-releases/accellion-responds-to-recent-fta-security-incident/

5. 聯絡資訊

如果您對此通告的內容有疑問或有關於此事件的建議，請勿直接回覆此信件，請以下述聯絡資訊與我們聯絡。

地 址：台北市富陽街 116 號

聯絡電話：02-27339922

傳真電話：02-27331655

電子郵件信箱：service@nccst.nat.gov.tw