行政院國家資通安全會報技術服務中心

中國駭客最常利用之 20 個漏洞資訊與修補方式

發布日	111/10/20

1. 概述

美國國家安全局(NSA)、網路安全暨基礎設施安全局(CISA)及聯邦調查局(FBI)共同公布自 2020 年迄今，最常遭到中國駭客利用之 20 個漏洞資訊與修補方式，呼籲各政府機關(構)與企業儘速修補下表之漏洞(依產品字母排序)。

項次	產品	CVE 編號
1	Apache APISIX	CVE-2022-24112
2	Apache HTTP Server	CVE-2021-41773
3	Apache Log4j	CVE-2021-44228
4	Atlassian Confluence Server and Data Center	CVE-2021-26084
5	Atlassian Confluence Server and Data Center	CVE-2022-26134
6	Buffalo WSR	CVE-2021-20090
7	Cisco Hyperflex HX	CVE-2021-1497
8	Citrix ADC	CVE-2019-19781
9	F5 Big-IP	CVE-2020-5902
10	F5 Big-IP	CVE-2022-1388
11	GitLab CE/EE	CVE-2021-22205
12	Hikvision Webserver	CVE-2021-36260
13	Microsoft Exchange	CVE-2021-26855
14	Microsoft Exchange	CVE-2021-26857

15	Microsoft Exchange	CVE-2021-26858
16	Microsoft Exchange	CVE-2021-27065
17	Pulse Connect Secure	CVE-2019-11510
18	Sitecore XP	CVE-2021-42237
19	VMware vCenter Server	CVE-2021-22005
20	ZOHO	CVE-2021-40539

2. 漏洞說明與修補方式

個別漏洞資訊與修補方式說明如下。

2.1.CVE-2022-24112

2.1.1. 漏洞說明

研究人員發現 Apache APISIX 存在安全漏洞(CVE-2022-24112)，攻擊者可藉由 batch-requests 外掛套件傳送惡意請求以繞過 Admin API 之 IP 限制，進而利用漏洞達成遠端執行任意程式碼，請儘速確認並進行更新。

2.1.2. 影響平台

Apache APISIX 2.10.4 與 2.12.1(不含)以下版本

2.1.3. 防護建議

- 請升級至 Apache APISIX 2.10.4 或 2.12.1(含)以上版本
- 如無法立即更新，請檢視 conf/config.yaml 之設定，若有啟用外掛套件(plugin)，可藉由關閉或註解 batch-requests 外掛套件以緩解此漏洞。

2.2.CVE-2021-41773

2.2.1. 漏洞說明

研究人員發現 Apache HTTP 伺服器存在安全漏洞(CVE-2021-41773)，攻擊者可藉由發送特製請求，利用此漏洞進而下載伺服器內任意檔案。

2.2.2. 影響平台

Apache HTTP Server 2.4.49 與 2.4.50 版本

2.2.3. 防護建議

目前 Apache 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或參考下列網址進行更新：

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

2.3.CVE-2021-44228

2.3.1. 漏洞說明

Apache Log4j 為一個 Java 日誌記錄工具，研究人員發現 Log4j 存在安全漏洞(CVE-2021-44228)，攻擊者可藉由發送特製 HTTP 請求觸發 JNDI 查詢功能，利用漏洞進而遠端執行任意程式碼，請儘速確認並進行更新。

2.3.2. 影響平台

Apache Log4j 2.0-beta9 至 2.14.1(含)版本

2.3.3. 防護建議

●Apache Log4j 官方網頁已針對此漏洞釋出更新程式(https://logging.apache.org/log4j/2.x/security.html)，請各機關聯絡設備維護廠商進行版本確認與更新：

– java6 Apache Log4j 請升級至 log4j 2.3.1(含)以上版本

– java7 Apache Log4j 請升級至 log4j 2.12.3(含)以上版本

– java8 Apache Log4j 請升級至 log4j 2.17.0(含)以上版本

●漏洞修補前，亦可透過以下步驟停用 JNDI Lookup 功能，以緩解此漏洞。

– 針對 log4j 版本>=2.10 的系統

➢請設定屬性「log4j2.formatMsgNoLookups=true」。

➢請設定環境變數「LOG4J_FORMAT_MSG_NO_LOOKUPS=true」。

– 針對 log4j 版本為 2.0-beta9 到 2.10.0 的系統

請自類別路徑(class path)中移除 JndiLookup.class。如執行下列指令，以自 log4j-core 中移除該類別：「zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class」。

●透過 WAF 對相關惡意語法進行過濾及阻擋

使用對外防護設備針對 JNDI 之相關惡意攻擊行為設定規則進行阻擋，例如”$(jndi:ldap://”。

●評估於 Java 伺服器增加以下設定以防止下載與執行可能具風險之惡意 Java Class。

將 com.sun.jndi.ldap.object.trustURLCodebase 設定為 false，使 JNDI 無法使用 LDAP 下載遠端 Codebase。

2.4.CVE-2021-26084

2.4.1. 漏洞說明

研究人員發現 Atlassian Confluence Server 與 Data Center 之 Webwork 模組存在安全漏洞(CVE-2021-26084)，攻擊者可在未經授權情況下對受影響伺服器進行 OGNL 注入攻擊，進而利用漏洞達成遠端執行任意程式碼，請儘速確

認並進行更新。

2.4.2. 影響平台

Atlassian Confluence Server 與 Data Center 6.13.23 以下、6.14.0 至 7.4.10、7.5.0 至 7.11.5 及 7.12.0 至 7.12.4(含)版本。

2.4.3. 防護建議

Atlassian 官方網頁已針對此漏洞釋出更新程式(https://jira.atlassian.com/browse/CONFSERVER-67940)，請各機關聯絡設備維護廠商進行版本確認並更新至 6.13.23、7.4.11、7.11.6、7.12.5 及 7.13.0(含)以上版本。

2.5.CVE-2022-26134

2.5.1. 漏洞說明

研究人員發現 Atlassian Confluence Server 與 Data Center 存在安全漏洞(CVE-2022-26134)，攻擊者可對受影響伺服器送出 Web 呼叫，在無憑證之情況下可取得伺服器權限並執行任意程式碼，請儘速確認並進行更新。

2.5.2. 影響平台

Atlassian Confluence Server 與 Data Center 1.3.0 至 7.4.16、7.13.0 至 7.13.6、7.14.0 至 7.14.2、7.15.0 至 7.15.1、7.16.0 至 7.16.3、7.17.0 至 7.17.3 及 7.18.0(含)版本。

2.5.3. 防護建議：

Atlassian 官方網站已針對此漏洞釋出更新程式(https://jira.atlassian.com/browse/CONFSERVER-79016)，請各機關聯絡設備維護廠商進行版本確認並更新至 7.4.17、7.13.7、7.14.3、7.15.2、7.16.4、

7.17.4 及 7.18.1(含)以上版本。

2.6.CVE-2021-20090

2.6.1. 漏洞說明

研究人員發現各廠牌路由器採用 Arcadyan firmware 公版路由器韌體程式之網頁控制介面存在安全漏洞(CVE-2021-20090)，攻擊者可透過傳送含有目錄遍歷字元之 URI 觸發此漏洞，即可繞過身分鑑別存取未經授權之頁面，請儘速確認並進行更新。

2.6.2. 影響平台

Tenable 已針對此漏洞列出受影響之路由器廠牌與產品型號(https://www.tenable.com/security/research/tra-2021-13)，採用 Arcadyan firmware 公版路由器韌體程式之路由器皆可能受到影響。

2.6.3. 防護建議

請各機關隨時注意原廠發表的更新訊息，並於原廠發表韌體更新程式釋出後，立即聯絡設備維護廠商進行版本確認及更新。

2.7.CVE-2021-1497

2.7.1. 漏洞說明

研究人員發現 Cisco HyperFlex HX 存在安全漏洞(CVE-2021-1497)，未經授權之遠端攻擊者可透過傳送特製請求至網頁管理介面觸發命令注入(Command injection)漏洞，並可透過 root 權限於受影響設備執行任意指令，請儘速確認並進行更新。

2.7.2. 影響平台

Cisco HyperFlex HX 4.0 與 4.5(含)之前的版本。

2.7.3. 防護建議

Cisco 官方網站已針對此漏洞釋出更新程式(https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hyperflex-rce-TjjNrkpR#fs)，請各機關聯絡設備維護廠商進行版本確認並更新 Cisco HyperFlex HX 至 4.0(2e)與 4.5(2a)(含)以上版本。

2.8.CVE-2019-19781

2.8.1. 漏洞說明

研究人員發現 Citrix Application Delivery Controller(以下簡稱 ADC)與 Gateway(原名稱為 NetScaler ADC 與 Gateway)存在目錄遍歷漏洞(CVE-2019-19781)，攻擊者可利用此漏洞於未經授權之情況下遠端執行任意程式碼，請儘速確認並進行更新。

2.8.2. 影響平台

●NetScaler ADC 與 NetScaler Gateway 10.5.70.12(不含)以下版本

●NetScaler ADC 與 NetScaler Gateway 11.1.63.15(不含)以下版本

●NetScaler ADC 與 NetScaler Gateway 12.0.63.13(不含)以下版本

●NetScaler ADC 與 NetScaler Gateway 12.1.55.18(不含)以下版本

●Citrix ADC 與 Citrix Gateway 13.0.47.24(不含)以下版本

●Citrix SD-WAN WANOP 設備型號 4000-WO、4100-WO、5000-WO 及 5100-WO 內之軟體 10.2.6b 與 11.0.3b 以下版本

2.8.3. 防護建議

Citrix 官方網站已針對此漏洞釋出更新程式(https://support.citrix.com/article/CTX267027/cve201919781-vulnerability-in-citrix-application-delivery-controller-citrix-gateway-and-citrix-sdwan-wanop-appliance)，請各機關聯絡設備維護廠商進行版本確認與更新：

●Citrix ADC 與 Gateway(原名稱為 NetScaler ADC 與 Gateway)請升級至 10.5.70.12、11.1.63.15、12.0.63.13、12.1.55.18 及 13.0.47.24(含)以上版本

●Citrix SD-WAN WANOP 請升級至 10.2.6b 與 11.0.3b(含)以上版本

2.9.CVE-2020-5902

2.9.1. 漏洞說明

研究人員發現 F5 Big-IP 存在安全漏洞(CVE-2020-5902)，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，請儘速確認並進行更新。

2.9.2. 影響平台：

●BIG-IP 11.6.1 至 11.6.5(含)版本

●BIG-IP 12.1.0 至 12.1.5(含)版本

●BIG-IP 13.1.0 至 13.1.3(含)版本

●BIG-IP 14.1.0 至 14.1.2(含)版本

●BIG-IP 15.1.0 與 15.0.0 版本

2.9.3. 防護建議

F5 官方網站已針對此漏洞釋出更新程式(https://support.f5.com/csp/article/K52145254)，請各機關聯絡設備維護廠商進

行版本確認並更新 BIG-IP 至 11.6.5.2、12.1.5.2、13.1.3.4、14.1.2.6、15.0.1.4、15.1.0.4 及 16.0.0(含)以上版本。

2.10.CVE-2022-1388

2.10.1. 漏洞說明

研究人員發現 F5 Networks 之 BIG-IP 產品存在高風險安全漏洞(CVE-2022-1388)，允許攻擊者繞過 iControl REST 元件之身分鑑別程序，進而存取 BIG-IP 系統，並遠端執行任意程式碼。

2.10.2. 影響平台

受影響之 BIG-IP(All modules)版本如下：

●11.6.1 至 11.6.5(含)版本

●12.1.0 至 12.1.6(含)版本

●13.1.0 至 13.1.4(含)版本

●14.1.0 至 14.1.4(含)版本

●15.1.0 至 15.1.5(含)版本

●16.1.0 至 16.1.2(含)版本

2.10.3. 防護建議

●目前 F5 官方已針對此漏洞釋出修復版本，請各機關可聯絡設備維護廠商或參考官方說明(https://support.f5.com/csp/article/K23605346)之「Security Advisory Status」一節進行更新：

– 連線至網址：https://support.f5.com/csp/knowledge-center/software/BIG-IP?module=BIG-IP%20LTM。

– 依所使用之模組與版本下載更新檔。

– 使用設備之管理頁面功能更新至最新版本。

●若目前所使用之版本因已停止支援而未釋出修補程式，建議升級至仍有支援且已推出修補程式之版本。

●若無法更新至最新版本，請參考 F5 官方網頁(https://support.f5.com/csp/article/K23605346)之「Mitigation」一節，採取緩解措施：

– 禁止透過設備之 self IP 位址存取 iControl REST 介面。

– 僅允許受信任之使用者與設備可透過 BIG-IP 設備管理頁面存取 iControl REST 介面。

– 調整 BIG-IP 設備之 httpd 設定檔。

2.11.CVE-2021-22205

2.11.1. 漏洞說明

研究人員發現 GitLab Community Edition(以下簡稱 CE)與 Enterprise Edition (以下簡稱 EE)使用之 ExifTool 開源工具存在安全漏洞(CVE-2021-22205)，攻擊者可上傳含有惡意指令之圖片即可觸發漏洞達成遠端執行任意程式碼，請儘速確認並進行更新。

2.11.2. 影響平台

●GitLab CE 與 EE 11.9.0 至 13.8.7(含)版本

●GitLab CE 與 EE 13.9.0 至 13.9.5(含)版本

●GitLab CE 與 EE 13.10.0 至 13.10.2(含)版本

2.11.3. 防護建議

GitLab 官方網站已針對此漏洞釋出更新程式(https://about.gitlab.com/releases/2021/04/14/security-release-gitlab-13-10-3-released/)，請各機關聯絡設備維護廠商進行版本確認並更新 GitLab CE 與 EE 至 13.8.8、13.9.6 或 13.10.3(含)以上版本。

2.12.CVE-2021-36260

2.12.1. 漏洞說明

研究人員發現中國監視攝影設備大廠海康威視 Hikvision 監視攝影機存在安全漏洞(CVE-2021-36260)，攻擊者可透過 SSH 連線，可傳送特製訊息進行命令注入攻擊取得 root shell，進而達成遠端執行任意程式碼，請儘速確認並進行更新。

2.12.2. 影響平台

受影響設備包含 IP 攝影機與 PTZ 攝影機共 70 餘款及部分網路監控主機(NVR)。韌體為 210628(含)以下版本之設備皆受到此漏洞影響，詳見 Hikvision 官方網頁公告之完整產品型號與版本(https://www.hikvision.com/en/support/cybersecurity/security-advisory/security-notification-command-injection-vulnerability-in-some-hikvision-products/)。

2.12.3. 防護建議

Hikvision 官方網頁已針對此漏洞釋出更新程式(https://www.hikvision.com/en/support/cybersecurity/security-advisory/security-notification-command-injection-vulnerability-in-some-hikvision-products/)，請各機關聯絡設備維護廠商進行版本確認與更新：

●請升級至 IPC_G3-V5.5.800 build 210628(含)以上版本

●請升級至 IPC H5-V5.5.800 build 210628(含)以上版本

2.13.CVE-2021-26855、CVE-2021-26857、CVE-2021-26858 及 CVE-2021-27065

2.13.1. 漏洞說明

研究人員發現 Microsoft Exchange Server 存在安全漏洞(CVE-2021-26855、CVE-2021-26857、CVE-2021-26858 及 CVE-2021-27065)，遠端攻擊者，透過與 Exchange Server 之 443 通訊埠建立連線並傳送特製封包而通過驗證，或者已具備 Exchange Server 登入帳號下，利用前述漏洞寫入任意檔案，進而達成遠端執行任意程式碼，請儘速確認並進行更新。

2.13.2. 影響平台

●Microsoft Exchange Server 2013

●Microsoft Exchange Server 2016

●Microsoft Exchange Server 2019

2.13.3. 防護建議

目前微軟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或參考以下網址進行更新：

●https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855

●https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26857

●https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26858

●https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-27065

2.14.CVE-2019-11510

2.14.1. 漏洞說明

研究人員發現 Pulse Connect Secure 存在安全漏洞(CVE-2019-11510)，攻擊者可以發送特製之 URI，在未經授權之情況下存取設備上任意檔案(如存放 VPN 帳號與密碼之檔案)，進而利用取得之認證資訊登入內部網路進行橫向移動，請儘速確認並進行更新。

2.14.2. 影響平台

●Pulse Connect Secure 8.2R1 至 8.2R12(含)版本

●Pulse Connect Secure 8.3R1 至 8.3R7(含)版本

●Pulse Connect Secure 9.0R1 至 9.0R3.3(含)版本

2.14.3. 防護建議：

Pulse Secure 官方網頁已針對此漏洞釋出更新程式(https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101/)，請各機關聯絡設備維護廠商進行版本確認與更新：

●Pulse Connect Secure 8.2RX 請升級至 8.2R12.1(含)以上版本

●Pulse Connect Secure 8.3RX 請升級至 8.3R7.1(含)以上版本

●Pulse Connect Secure 9.0RX 請升級至 9.0R3.4 或 9.0R4(含)以上版本

2.15.CVE-2021-42237

2.15.1. 漏洞說明

研究人員發現 Sitecore Experience Platform(Sitecore XP)存在不安全反序列化漏洞(CVE-2021-42237)，攻擊者可於未經授權與特殊設定之情況下，利用漏

洞達成遠端執行任意程式碼，請儘速確認並進行更新。

2.15.2. 影響平台

●Sitecore XP 7.5 初始版本至 Sitecore XP 7.5 Update-2(含)版本

●Sitecore XP 8.0 初始版本至 Sitecore XP 8.0 Update-7(含)版本

●Sitecore XP 8.1 初始版本至 Sitecore XP 8.1 Update-3(含)版本

●Sitecore XP 8.2 初始版本至 Sitecore XP 8.2 Update-7(含)版本

2.15.3. 防護建議

Sitecore 官方網頁已針對此漏洞釋出更新程式(https://support.sitecore.com/kb?id=kb_article_view&sysparm_article=KB1000776)，請各機關聯絡設備維護廠商進行版本確認與更新：

●Sitecore XP 7.5.0 至 Sitecore XP 7.5.2，請採取下列其中一種防護措施：

– 升級至 Sitecore XP 9.0.0(含)以上版本

– 移除所有伺服器上之 Report.ashx 檔案(路徑為：/sitecore/shell/ClientBin/Reporting/Report.ashx)。

●Sitecore XP 8.0.0 至 Sitecore XP 8.2.7 防護方式

移除所有伺服器上之 Report.ashx 檔案(路徑為：/sitecore/shell/ClientBin/Reporting/Report.ashx)

2.16.CVE-2021-22005

2.16.1. 漏洞說明

研究人員發現 VMware vCenter Server 存在安全漏洞(CVE-2021-22005)，攻擊者可透過上傳特製檔案至 vCenter 伺服器 443 連接埠，即可透過該檔案利

用漏洞執行程式碼，請儘速確認並進行更新。

2.16.2. 影響平台

●vCenter Server 6.7 版本至 6.7 U3o(不含)版本

●vCenter Server 7.0 版本至 7.0 U2d(不含)版本

●Cloud Foundation (vCenter Server) 3.0 版本至 3.10.2.2(不含)版本

●Cloud Foundation (vCenter Server) 4.0 版本至 4.3.1(不含)版本

2.16.3. 防護建議

VMware 官方網站已針對此漏洞釋出更新程式(https://kb.vmware.com/s/article/85717)，請各機關聯絡設備維護廠商進行版本確認與更新：

●vCenter Server 請升級至 6.7 U3o 與 7.0 U2c(含)以上版本

●Cloud Foundation(vCenter Server)請升級至 3.10.2.2 與 4.3.1(含)以上版本

2.17.CVE-2021-40539

2.17.1. 漏洞說明

研究人員發現 Zoho ManageEngine ADSelfService Plus 存在安全漏洞(CVE-2021-40539)，攻擊者可藉由特製之 Rest API URL 利用漏洞繞過身份鑑別，進而達成遠端執行任意程式碼，請儘速確認並進行更新。

2.17.2. 影響平台

ManageEngine ADSelfService Plus build 6113(含)以下版本

2.17.3. 防護建議

ManageEngine 官方網站已針對此漏洞釋出更新程式(https://www.manageengine.com/products/self-service-password/advisory/CVE-2021-40539.html)，請各機關聯絡設備維護廠商進行版本確認並更新至ManageEngine ADSelfService Plus build 6114(含)以上版本。

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 及 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 與 Java)更新情況，並定期檢視系統與應用程式更新紀錄，避免駭客利用系統或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) 透過專職監控人員或自動化機制即時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，宣導使用者留意相關電子郵件，注意郵件之來源的正確性，勿開啟不明來源信件的附檔或連結。

(7) 建立良好之網段管理機制，確保隔離網段可獨立運行。

(8) 利用第三方滲透測試，確認系統安全性與強化防護能量。

4. 參考資料

[1]https://www.cisa.gov/uscert/ncas/alerts/aa22-279a

[2]https://lists.apache.org/thread/lcdqywz8zy94mdysk7p3gfdgn51jmt94

[3]https://httpd.apache.org/security/vulnerabilities_24.html

[4]https://logging.apache.org/log4j/2.x/security.html

[5]https://jira.atlassian.com/browse/CONFSERVER-67940

[6]https://jira.atlassian.com/browse/CONFSERVER-79016

[7]https://www.tenable.com/security/research/tra-2021-13

[8]https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hyperflex-rce-TjjNrkpR#fs

[9]https://support.citrix.com/article/CTX267027/cve201919781-vulnerability-in-citrix-application-delivery-controller-citrix-gateway-and-citrix-sdwan-wanop-appliance

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

[11]https://support.f5.com/csp/article/K23605346

[12]https://about.gitlab.com/releases/2021/04/14/security-release-gitlab-13-10-3-released/

[13]https://www.hikvision.com/en/support/cybersecurity/security-advisory/security-notification-command-injection-vulnerability-in-some-hikvision-products/

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

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

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

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

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

[19]https://support.sitecore.com/kb?id=kb_article_view&sysparm_article=KB1000776

[20]https://kb.vmware.com/s/article/85717

[21]https://www.manageengine.com/products/self-service-password/advisory/CVE-2021-40539.html

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