

張貼日期：2026/10/05

【漏洞預警】CISA新增12個已知遭駭客利用之漏洞至KEV目錄(2026/09/21-2026/09/27)

- 主旨說明: 【漏洞預警】CISA新增12個已知遭駭客利用之漏洞至KEV目錄(2026/09/21-2026/09/27)
- 內容說明:
 - 轉發 台灣電腦網路危機處理暨協調中心 資安訊息警訊 TWCERTCC-200-202610-00000001
 - 【CVE-2026-7273】Zyxel GS1900 Series Switches Stack-Based Buffer Overflow Vulnerability (CVSS v3.1: 8.8)
 - 【是否遭勒索軟體利用:未知】 Zyxel GS1900系列交換器的CGI程式存在堆疊型緩衝區溢位漏洞，可能使未經驗證的區域網路攻擊者透過特製的HTTP請求執行作業系統指令。
 - 【CVE-2026-93952】Arista VeloCloud Orchestrator Improper Input Validation Vulnerability (CVSS v3.1: 10.0)
 - 【是否遭勒索軟體利用:未知】 Arista VeloCloud Orchestrator本地部署版本存在輸入驗證不當漏洞，可能允許遠端攻擊者存取具特權的內部功能，可能危及Orchestrator及其所管理資料的機密性、完整性與可用性。
 - 【CVE-2026-94127】F5 BIG-IP APM Heap-based Buffer Overflow Vulnerability (CVSS v3.1: 9.8)
 - 【是否遭勒索軟體利用:未知】 F5 BIG-IP APM存在堆積型緩衝區溢位漏洞。當虛擬伺服器設定存取原則及OAuth設定檔時，未經驗證的攻擊者可能利用此漏洞實現遠端程式碼執行。
 - 【CVE-2026-93616】Check Point Multiple Products Path Traversal Vulnerability (CVSS v3.1: 9.8)
 - 【是否遭勒索軟體利用:未知】 Check Point Security Management Server、Multi-Domain Security Management Server、Log Server、Multi-Domain Log Server及SmartEvent存在路徑遍歷漏洞，可能允許未經驗證的攻擊者上傳並執行任意指令碼。
 - 【CVE-2026-85102】Check Point Multiple Products Improper Certificate Validation Vulnerability (CVSS v3.1: 9.8)
 - 【是否遭勒索軟體利用:未知】 Check Point Security Gateway及使用Site-to-Site VPN或Remote Access VPN的Check Point Spark Firewall存在憑證驗證不當漏洞，可能允許未經驗證的遠端攻擊者在Gateway上執行任意程式碼。
 - 【CVE-2026-5430】WSO2 Multiple Products Path Traversal Vulnerability (CVSS v3.1: 10.0)
 - 【是否遭勒索軟體利用:未知】 WSO2 API Control Plane、API Manager、Traffic Manager及Universal Gateway存在路徑遍歷漏洞，可能允許不受限制的檔案上傳，進而導致遠端程式碼執行。
 - 【CVE-2026-71362】Adobe Commerce and Magento Incorrect Authorization Vulnerability (CVSS v3.1: 9.1)
 - 【是否遭勒索軟體利用:未知】 Adobe Commerce和Magento存在授權不當漏洞，可能允許攻擊者在無需任何使用者互動的情況下，以更高的權限存取敏感資源。
 - 【CVE-2026-67279】Mikrotik RouterOS Improper Enforcement of Behavioral Workflow Vulnerability (CVSS v3.1: 6.5)
 - 【是否遭勒索軟體利用:未知】 MikroTik RouterOS 存在行為流程強制執行不當漏洞，可能允許未經身分驗證的用戶端開啟工作階段通道並傳送執行請求。
 - 【CVE-2026-65660】Microsoft SharePoint Code Injection Vulnerability (CVSS v3.1: 8.8)
 - 【是否遭勒索軟體利用:未知】 Microsoft SharePoint 存在程式碼注入漏洞，可能允許經授權的攻擊者透過網路執行程式碼。
 - 【CVE-2026-87902】WordPress Core Remote File Inclusion Vulnerability (CVSS v3.1: 8.1)

- 【是否遭勒索軟體利用:未知】WordPress Core存在遠端檔案包含漏洞，可能允許未經驗證的攻擊者讓頁面範本解析機制包含可讀取的本機.php檔案，進而導致遠端程式碼執行。
- [CVE-2026-88772]Citrix NetScaler Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability (CVSS v3.1: 8.1)
- 【是否遭勒索軟體利用:未知】Citrix NetScaler ADC 和 NetScaler Gateway 存在記憶體緩衝區內操作限制不當漏洞，可能允許攻擊者遠端執行程式碼或導致阻斷服務。
- [CVE-2026-88771]Citrix NetScaler Improper Input Validation Vulnerability (CVSS v3.1: 9.8)
- 【是否遭勒索軟體利用:未知】Citrix NetScaler ADC 和 NetScaler Gateway存在輸入驗證不當漏洞，可能允許未經驗證的攻擊者執行任意指令。
- 影響平台:
 - [CVE-2026-7273]請參考官方所列的影響版本
<https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-stack-based-buffer-overflow-vulnerability-in-gs1900-series-switches-06-16-2026>
 - [CVE-2026-93952]請參考官方所列的影響版本
<https://www.arista.com/en/support/advisories-notice/security-advisory/24765-security-advisory-0183>
 - [CVE-2026-94127]請參考官方所列的影響版本
<https://my.f5.com/manage/s/article/K000162605>
 - [CVE-2026-93616]請參考官方所列的影響版本
<https://support.checkpoint.com/results/sk/sk1000171/>
 - [CVE-2026-85102]請參考官方所列的影響版本
<https://support.checkpoint.com/results/sk/sk1000117>
 - [CVE-2026-5430]請參考官方所列的影響版本
<https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2026/WSO2-2026-5328/>
 - [CVE-2026-71362]請參考官方所列的影響版本
<https://www.adobe.com/trust/security/products/commerce/apsb26-92.html>
 - [CVE-2026-67279]請參考官方所列的影響版本
<https://mikrotik.com/supportsec/september-2026-vulnerability/>
 - [CVE-2026-65660]請參考官方所列的影響版本
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65660>
 - [CVE-2026-87902]請參考官方所列的影響版本
<https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-7hp8-65ch-5w-hp>
 - [CVE-2026-88772]請參考官方所列的影響版本
<https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697096>
 - [CVE-2026-88771]請參考官方所列的影響版本
<https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697096>
- 建議措施:
 - [CVE-2026-7273] 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-stack-based-buffer-overflow-vulnerability-in-gs1900-series-switches-06-16-2026>
 - [CVE-2026-93952] 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://www.arista.com/en/support/advisories-notice/security-advisory/24765-security-advisory-0183>
 - [CVE-2026-94127] 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://my.f5.com/manage/s/article/K000162605>
 - [CVE-2026-93616] 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://support.checkpoint.com/results/sk/sk1000171/>
 - [CVE-2026-85102] 官方已針對漏洞釋出修復更新，請更新至相關版本

<https://support.checkpoint.com/results/sk/sk1000117>

- [CVE-2026-5430] 官方已針對漏洞釋出修復更新，請更新至相關版本

<https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2026/WSO2-2026-5328/>

- [CVE-2026-71362] 官方已針對漏洞釋出修復更新，請更新至相關版本

<https://www.adobe.com/trust/security/products/commerce/apsb26-92.html>

- [CVE-2026-67279] 官方已針對漏洞釋出修復更新，請更新至相關版本

<https://mikrotik.com/supportsec/september-2026-vulnerability/>

- [CVE-2026-65660] 官方已針對漏洞釋出修復更新，請更新至相關版本

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65660>

- [CVE-2026-87902] 官方已針對漏洞釋出修復更新，請更新至相關版本

<https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-7hp8-65ch-5w hp>

- [CVE-2026-88772] 官方已針對漏洞釋出修復更新，請更新至相關版本

<https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697096>

- [CVE-2026-88771] 官方已針對漏洞釋出修復更新，請更新至相關版本

<https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697096>

- 參考資料:

計算機與通訊中心
網路系統組 敬啟

From:

<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:

https://net.nthu.edu.tw/netsys/mailling:announcement:20261005_21

Last update: **2026/10/05 12:16**

