

來源: service <service@cert.tanet.edu.tw>

收信: service@cert.tanet.edu.tw

日期: Wed, 21 Oct 2026 10:07:56

(ANA事件單通知:TACERT-ANA-2026102109105656)(【漏洞預

標題: 警】CISA新增9個已知遭駭客利用之漏洞至KEV目錄
(2026/10/12-2026/10/18))

附檔: [00.html](#) (7k)

教育機構ANA通報平台

發佈 編號	TACERT-ANA-2026102109105656	發佈 時間	2026-10-21 09:51:57
事故 類型	ANA-漏洞預警	發現 時間	2026-10-21 09:51:57
影響 等級	低		

[主旨說明:] 【漏洞預警】CISA新增9個已知遭駭客利用之漏洞至KEV目錄(2026/10/12-2026/10/18)

[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-200-202610-00000029

【CVE-2026-104935】 Ivanti Connect Secure Authentication Bypass by Spoofing Vulnerability (CVSS v3.1: 8.6)

【是否遭勒索軟體利用:未知】 Ivanti Connect Secure 存在身分鑑別繞過漏洞，允許遠端未經身分驗證的攻擊者執行任意指令。

【CVE-2026-96951】 Microsoft Windows Command Injection Vulnerability (CVSS v3.1: 8.8)

【是否遭勒索軟體利用:未知】 Microsoft Windows Shell 存在指令注入漏洞，未經授權的攻擊者可透過網路繞過安全性功能。

【CVE-2026-105134】 Ahsay AhsayCBS Command Injection Vulnerability (CVSS v3.1: 10.0)

【是否遭勒索軟體利用:未知】 Ahsay AhsayCBS 存在指令注入漏洞，遠端攻擊者可透過操控 Replication Receiver 元件中 /rps/api/json/UpdateReceivers.do 端點的隨機參數來執行作業系統指令。

【CVE-2026-76519】 Cisco Secure Email Gateway Relative Path Traversal Vulnerability (CVSS v3.1: 9.8)

【是否遭勒索軟體利用:未知】 Cisco Secure Email Gateway 存在相對路徑遍歷漏洞，未經身分驗證的遠端攻擊者可利用此漏洞，在底層作業系統中寫入任意檔案。

【CVE-2026-105133】 Ahsay AhsayCBS Improper Authentication Vulnerability (CVSS v3.1: 7.3)

【是否遭勒索軟體利用:未知】 Ahsay AhsayCBS 存在不當驗證漏洞，遠端攻擊者可透過操控 API 元件中 checkSysPwd 函式的隨機參數來繞過驗證機制。

【CVE-2026-0322】Palo Alto Networks PAN-OS Code Injection Vulnerability (CVSS v3.1: 7.2)
【是否遭勒索軟體利用:未知】 Palo Alto Networks PAN-OS 存在程式碼注入漏洞，具網路存取權限且已通過身分驗證的攻擊者，可利用此漏洞在防火牆上以 root 權限執行任意程式碼。

【CVE-2026-21589】Atlassian Multiple Products Files or Directories Accessible to External Parties Vulnerability (CVSS v4.0: 9.3)
【是否遭勒索軟體利用:未知】 多款 Atlassian 產品存在檔案或目錄可被外部人員存取的漏洞，可能導致未經身分驗證的攻擊者在受影響版本中存取Web 應用程式根目錄內的特定檔案。

【CVE-2026-102764】BeyondTrust Remote Support Authentication Bypass by Spoofing Vulnerability (CVSS v3.1: 9.8)
【是否遭勒索軟體利用:未知】 BeyondTrust Remote Support 存在身分鑑別繞過漏洞，可能使遠端攻擊者得以在設備上執行檔案操作。

【CVE-2025-61624】Fortinet Multiple Products Path Traversal Vulnerability (CVSS v3.1: 6.0)
【是否遭勒索軟體利用:未知】 FortiOS、FortiPAM、FortiProxy 及 FortiSwitchManager 存在路徑遍歷漏洞，具有管理員身分且至少具備讀寫權限的已驗證攻擊者，可能透過特定的 CLI 指令寫入或刪除任意檔案。

情資分享等級: WHITE(情資內容為可公開揭露之資訊)
此訊息僅發送到「區縣市網路中心」，煩請貴單位協助轉發與通知轄下各單位知悉

[影響平台:]

【CVE-2026-104935】請參考官方所列的影響版本 <https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-CVE-2026-104935>

【CVE-2026-96951】請參考官方所列的影響版本 <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-96951>

【CVE-2026-105134】請參考官方所列的影響版本 <https://www.ahsay.com/en/support/help-centre/release-notes/cbs/v10.3.4>

【CVE-2026-76519】請參考官方所列的影響版本 <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-afw-zqYJkjxp>

【CVE-2026-105133】請參考官方所列的影響版本 <https://www.ahsay.com/en/support/help-centre/release-notes/cbs/v10.3.4>

【CVE-2026-0322】請參考官方所列的影響版本 <https://security.paloaltonetworks.com/CVE-2026-0322>

【CVE-2026-21589】請參考官方所列的影響版本 <https://confluence.atlassian.com/security/cve-2026-21589-arbitrary-file-access-vulnerability-impacts-multiple-products-1870495748.html>

【CVE-2026-102764】請參考官方所列的影響版本 <https://www.beyondtrust.com/blog/entry/bt26-05>

【CVE-2025-61624】請參考官方所列的影響版本 <https://fortiguard.fortinet.com/psirt/FG-IR-26-122>

[建議措施:]

【CVE-2026-104935】 官方已針對漏洞釋出修復更新，請更新至相關版本 <https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-CVE-2026-104935>

【CVE-2026-96951】 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-2026-96951>

【CVE-2026-105134】 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://www.ahsay.com/en/support/help-centre/release-notes/cbs/v10.3.4>

【CVE-2026-76519】 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-afw-zqYJkjpg>

【CVE-2026-105133】 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://www.ahsay.com/en/support/help-centre/release-notes/cbs/v10.3.4>

【CVE-2026-0322】 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://security.paloaltonetworks.com/CVE-2026-0322>

【CVE-2026-21589】 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://confluence.atlassian.com/security/cve-2026-21589-arbitrary-file-access-vulnerability-impacts-multiple-products-1870495748.html>

【CVE-2026-102764】 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://www.beyondtrust.com/blog/entry/bt26-05>

【CVE-2025-61624】 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://fortiguard.fortinet.com/psirt/FG-IR-26-122>

[參考資料:]

(此通報僅在於告知相關資訊，並非為資安事件)，如果您對此通報的內容有疑問或有關於此事件的建議，歡迎與我們連絡。

教育機構資安通報應變小組

網址：<https://info.cert.tanet.edu.tw/>

專線電話：07-5250211

網路電話：98400000

E-Mail：service@cert.tanet.edu.tw