

教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2026091801090909	發佈時間	2026-09-18 13:34:10
事故類型	ANA-漏洞預警	發現時間	2026-09-18 13:34:10
影響等級	中		
[主旨說明:] 【漏洞預警】 HPE Aruba Networking AOS-CX 存在 6 個高風險安全漏洞，請儘速確認並進行修補			
[內容說明:] 轉發 國家資安資訊分享與分析中心 資安訊息警訊 NISAC-200-202609-00000014 研究人員發現 HPE Aruba Networking AOS-CX 存在 6 個高風險安全漏洞(CVE-2026-73749 至 CVE-2026-73753 與 CVE-2026-73782)，類型包含不當存取控制(Improper Access Control)、指令注入(Command Injection)、路徑遍歷(Path Traversal)、作業系統指令注入(OS Command Injection)及使用外部控制之格式化字串(Use of Externally-Controlled Format String)。其中最嚴重之漏洞可使未經身分鑑別之遠端攻擊者，藉由對受影響服務傳送特製封包，進而以較高權限執行任意程式碼，請儘速確認並進行修補。 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:] AOS-CX 10.18.0001 版本 AOS-CX 10.17.1021(含)以前版本			

AOS-CX 10.16.1051(含)以前版本

AOS-CX 10.13.1180(含)以前版本

AOS-CX 10.10.1180(含)以前版本

[建議措施:]

官方已針對漏洞釋出修補或更新，請參考官方說明進行處置，網址如下：

https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05134en_us&docLocale=en_US

[參考資料:]

1. <https://nvd.nist.gov/vuln/detail/CVE-2026-73749>

2. <https://nvd.nist.gov/vuln/detail/CVE-2026-73750>

3. <https://nvd.nist.gov/vuln/detail/CVE-2026-73751>

4. <https://nvd.nist.gov/vuln/detail/CVE-2026-73752>

5. <https://nvd.nist.gov/vuln/detail/CVE-2026-73753>

6. <https://nvd.nist.gov/vuln/detail/CVE-2026-73782>

7.

https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05134en_us&docLocale=en_US