1140505-1140511 各大廠牌軟硬體高風險弱點摘要				
廠牌	軟硬體型號	弱點數量	說明	CVE ID
Arista Networks	CloudVision Portal	1	在受影響版本的 CloudVision Portal 中，不當的存取控制可能使惡意的已驗證使用者能夠對受管的 EOS 裝置執行超出原本授權範圍的操作。 此資安公告影響的是**部署於本地（on-premise）**的 Arista CloudVision Portal 產品，不影響 CloudVision as-a-Service（雲端版本）。	CVE-2024-11186
Arista Networks	CloudVision Portal	1	在 Arista CloudVision 系統（包括虛擬或實體的本地部署）中，零接觸佈建（Zero Touch Provisioning, ZTP）可能被用來在 CloudVision 系統上取得超出必要範圍的管理員權限。攻擊者可藉此查詢或操控受管設備的系統狀態。 請注意，此漏洞不影響 CloudVision as-a-Service（雲端版本）。	CVE-2025-0505
Arista Networks	CloudVision Portal	1	在受影響的 Arista EOS 平台上，若已設定 secure VxLAN，當 Tunnelsec agent 被重新啟動時，封包會在 secure VxLAN 通道中以明文形式傳送，導致資料可能被攔截。 這表示在特定情況下，原應加密的通訊資料會因代理程式重啟而暫時失去保護，造成潛在的資訊洩漏風險。	CVE-2024-12378
Arista Networks	EOS	1	在受影響的 Arista EOS 平台上，若已設定 **Traffic Policies（流量策略）**，此漏洞將導致**接收到的未標記封包（untagged packets）無法符合原本應該匹配的流量策略規則**。 例如： 若某條規則應該**丟棄特定封包**，該封包卻不會被丟棄，反而會像沒有這條規則一樣被**正常轉發**，這可能導致封包被傳送到**意料之外的目的地**，造成潛在的安全風險或流量繞過。	CVE-2024-9448
Cisco	Cisco Adaptive Security Appliance (ASA) Software	1	在 Cisco Adaptive Security Appliance (ASA) 軟體、Cisco Firepower Threat Defense (FTD) 軟體、Cisco IOS 與 IOS XE 軟體中，Internet Key Exchange version 2 (IKEv2) 協定處理存在一個漏洞。該漏洞可能允許未經身份驗證的遠端攻擊者對受影響的設備造成**阻斷服務（DoS）**狀況。	CVE-2025-20182
Cisco	Cisco Catalyst SD-WAN Manager	1	在 Cisco Catalyst SD-WAN Manager（前稱 Cisco SD-WAN vManage）的 CLI 中發現了一個漏洞，可能允許已驗證的本地攻擊者在底層作業系統上取得 root 權限。建議儘快更新至修補版本，以防止潛在的權限提升攻擊。	CVE-2025-20122
Cisco	Cisco Digital Network Architecture Center (DNA Center)	1	在 Cisco Catalyst Center（前稱 Cisco DNA Center）的管理 API 中發現一個漏洞，可能允許未經身份驗證的遠端攻擊者讀取及修改對外 Proxy 設定。此漏洞風險等級高，建議立即評估影響範圍並套用 Cisco 提供的修補措施。	CVE-2025-20210

Cisco	Cisco IOS XE Software	1	在 Cisco IOS XE 軟體的 Wireless LAN Controllers（WLCs）中，Out-of-Band AP Image Download 功能存在一項漏洞，可能允許未經身份驗證的遠端攻擊者向受影響系統上傳任意檔案。此漏洞可能導致完整系統接管，建議立即檢查是否啟用該功能，並採取官方建議的修補或緩解措施。	CVE-2025-20188
Cisco	Cisco IOS XE Software	1	Cisco IOS XE 軟體中的 DHCP snooping 安全功能 存在一項漏洞，可能允許未經身份驗證的遠端攻擊者造成介面的封包佇列完全塞住（queue wedge），導致**阻斷服務（DoS）**狀況。此漏洞具有高風險，建議 Cisco 使用者檢查是否受影響並儘快套用修補或緩解措施。	CVE-2025-20162
Cisco	Cisco IOS XE Software	1	Cisco IOS XE 軟體中 Wireless LAN Controller 功能 的網頁管理介面存在一項漏洞，可能允許已驗證的遠端攻擊者（擁有 lobby ambassador 使用者帳戶）對受影響的設備執行指令注入攻擊。此漏洞可能導致完整系統控制權被取得。建議： 檢查是否啟用 lobby ambassador 帳戶 限制該帳戶的存取 儘快套用 Cisco 官方提供的修補程式	CVE-2025-20186
Cisco	Cisco IOS XE Software	1	無線區域網路控制器 (WLC) 的 Cisco IOS XE 軟體的無線網路控制守護程式 (wncd) 中存在弱點，可能允許未經身份驗證的相鄰無線攻擊者導致阻斷服務 (DoS) 情況。此弱點是由於記憶體管理不當造成的。攻擊者可以透過從關聯的無線 IPv6 用戶端向受影響的裝置發送一系列 IPv6 網路請求來利用此弱點。為了將客戶端關聯到設備，攻擊者可能首先需要對網路進行身份驗證，或者在配置的開放網路的情況下自由關聯。成功利用該弱點可以讓攻擊者導致 wncd 進程消耗可用記憶體並最終導致裝置停止回應，從而導致 DoS 情況。	CVE-2025-20140
Cisco	Cisco IOS XE Software	1	在具有路由交換處理器 3 (RSP3C) 的 Cisco ASR 903 聚合服務路由器的 Cisco IOS XE 軟體的 Cisco Express Forwarding 功能中存在弱點，可能允許未經驗證的相鄰攻擊者觸發阻斷服務 (DoS) 條件。此弱點是由於 Cisco IOS XE 軟體在處理位址解析協定 (ARP) 訊息時記憶體管理不當所造成的。攻擊者可以透過在一段時間內以高速率向受影響的裝置發送精心設計的 ARP 訊息來利用此弱點。成功利用弱點可能會使攻擊者耗盡系統資源，最終觸發活動路由交換處理器 (RSP) 的重新載入。如果不存在冗餘 RSP，則路由器將重新載入。	CVE-2025-20189
Cisco	Cisco IOS XE Software	1	Cisco IOS XE 軟體的 Internet 金鑰交換版本 1 (IKEv1) 實作中存在弱點，可能允許經過驗證的遠端攻擊者造成阻斷服務 (DoS) 情況。攻擊者必須擁有有效的 IKEv1 VPN 憑證才能利用此弱點。此弱點是由於在將 IPsec 安全關聯建立請求傳遞給受影響設備的硬體加密加速器之前對 IKEv1 第 2 階段參數的驗證不當造成的。攻擊者可以透過向受影響的裝置	CVE-2025-20192

			發送精心設計的 IKEv1 訊息來利用此弱點。成功利用該弱點可使攻擊者導致設備重新載入。	
Cisco	Cisco IOS XE Software	1	Cisco IOS XE 無線控制器軟體中的弱點可能允許未經驗證的相鄰攻擊者在受影響的裝置上導致阻斷服務 (DoS) 情況。此弱點是由於無線控制器處理存取點 (AP) 思科發現協定 (CDP) 鄰居報告時輸入驗證不足所造成的。攻擊者可以透過向 AP 發送精心設計的 CDP 封包來利用此弱點。成功利用該弱點可能使攻擊者導致管理 AP 的無線控制器意外重新加載，從而導致影響無線網路的 DoS 情況。	CVE-2025-20202
Cisco	Cisco IOS XR Software	1	Cisco IOS 軟體和 Cisco IOS XE 軟體的雙向主動測量協定 (TWAMP) 伺服器功能中存在弱點，可能允許未經驗證的遠端攻擊者導致受影響的裝置重新載入，從而導致阻斷服務 (DoS) 情況。對於 Cisco IOS XR 軟體，如果啟用偵錯，此弱點可能導致 ipsla_ippm_server 程序意外重新載入。此弱點是由於處理特製的 TWAMP 控制封包時發生越界數組存取所造成的。攻擊者可以透過向受影響的裝置發送精心設計的 TWAMP 控制封包來利用此弱點。成功利用該弱點可使攻擊者導致受影響的設備重新加載，從而導致 DoS 情況。注意：對於 Cisco IOS XR 軟體，只有 ipsla_ippm_server 程序會意外重新載入，並且僅在啟用偵錯時才會發生。 Cisco IOS XR 軟體的弱點詳情如下： 安全影響等級 (SIR)：低 CVSS 基本分數：3.7 CVSSSS;向量：CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L	CVE-2025-20154
Cisco	Cisco NX-OS Software	1	Cisco IOS 軟體、Cisco IOS XE 軟體、Cisco NX-OS 軟體和 Cisco 無線區域網路控制器 (WLC) AireOS 軟體的交換器整合安全功能 (SISF) 中存在弱點，可能允許未經驗證的相鄰攻擊者在受影響的裝置上造成阻斷服務 (DoS) 情況。此弱點是由於對 DHCPv6 封包的錯誤處理造成的。攻擊者可以透過向受影響的裝置發送精心設計的 DHCPv6 封包來利用此弱點。成功利用該弱點可使攻擊者導致設備重新加載，從而導致 DoS 情況。	CVE-2025-20191
Cisco	IOS	1	Cisco IOS 軟體的 Cisco 工業乙太網路交換器設備管理員 (DM) 中存在弱點，可能允許經過驗證的遠端攻擊者提升權限。此弱點是由於對經過身份驗證的使用者的授權驗證不足所造成的。攻擊者可以透過向受影響的裝置發送精心設計的 HTTP 請求來利用此弱點。成功利用弱點可使攻擊者將權限提升至權限等級 15	CVE-2025-20164
D-Link	DIR-600L	1	在 D-Link DIR-600L 2.07B01 版本中發現了一個被列為嚴重弱點。受此問題影響的是函數 formEasySetupWizard3。對參數主機的操縱導致緩衝區溢	CVE-2025-4342

			位。攻擊可能是遠端發起的。此弱點僅影響維護者不再支援的產品。	
D-Link	DIR-600L	1	在 D-Link DIR-600L 2.07B01 版本中發現一個弱點，該弱點被歸類為嚴重弱點。此弱點影響 EasySetupWizard 函數。對參數主機的操縱導致緩衝區溢位。攻擊可以遠端發動。此弱點僅影響維護者不再支援的產品。	CVE-2025-4343
D-Link	DIR-600L	1	在 D-Link DIR-600L 2.07B01 版本中發現了一個弱點，該弱點被歸類為嚴重弱點。這會影響功能 formLogin。對參數主機的操縱導致緩衝區溢位。可以遠端發動攻擊。此弱點僅影響維護者不再支援的產品。	CVE-2025-4344
D-Link	DIR-600L	1	在 D-Link DIR-600L（最高版本為 2.07B01）中發現一個漏洞，並被歸類為重大。此問題影響 `formSetLog` 函數。對引數 host 的操作會導致緩衝區溢位。攻擊可能從遠端發起。此漏洞僅影響已不再由維護者支援的產品。	CVE-2025-4345
D-Link	DIR-600L	1	在 D-Link DIR-600L（最高版本為 2.07B01）中發現一個漏洞。它已被歸類為重大。受影響的函數為 `formSetWAN_Wizard534`。對引數 host 的操作會導致緩衝區溢位。此攻擊可以從遠端發起。此漏洞僅影響已不再由維護者支援的產品。	CVE-2025-4346
D-Link	DIR-600L	1	在 D-Link DIR-600L（最高版本為 2.07B01）中發現一個漏洞。它已被宣告為重大。此漏洞影響的函數為 `formWlSiteSurvey`。對引數 host 的操作會導致緩衝區溢位。攻擊可由遠端發起。此漏洞僅影響已不再由維護者支援的產品。	CVE-2025-4347
D-Link	DIR-600L	1	在 D-Link DIR-600L（最高版本為 2.07B01）中發現一個漏洞。它已被評為重大。此問題影響的函數為 `formSetWanL2TP`。對引數 host 的操作會導致緩衝區溢位。攻擊可能從遠端發起。此漏洞僅影響已不再由維護者支援的產品。	CVE-2025-4348
D-Link	DIR-600L	1	在 D-Link DIR-600L（最高版本為 2.07B01）中發現一個被歸類為重大等級的漏洞。此漏洞影響 `formSysCmd` 函數。對引數 host 的操作會導致命令注入。攻擊可能從遠端發起。此漏洞僅影響已不再由維護者支援的產品。	CVE-2025-4349
D-Link	DIR-600L	1	在 D-Link DIR-600L（最高版本為 2.07B01）中發現一個被歸類為「重大」的漏洞。此漏洞影響 `wake_on_lan` 函數。對引數 `host` 的操作會導致命令注入。攻擊可從遠端發起。此漏洞僅影響已不再由維護者支援的產品。	CVE-2025-4350
D-Link	DIR-605L	1	在 D-Link DIR-605L（版本 2.13B01）中發現一個漏洞，並已被歸類為「重大」。此漏洞影響 `formSetWAN_Wizard534` 函數。對引數 `curTime`	CVE-2025-4441

			的操作會導致緩衝區溢位。攻擊可能從遠端發起。供應商已在此漏洞披露初期被通知。此漏洞僅影響已不再由維護者支援的產品。	
D-Link	DIR-605L	1	在 D-Link DIR-605L（版本 2.13B01）中發現一個漏洞，並已被宣告為「重大」。此漏洞影響 `formSetWAN_Wizard55` 函數。對引數 `curTime` 的操作會導致緩衝區溢位。攻擊可從遠端發起。供應商已在此漏洞披露初期被通知。此漏洞僅影響已不再由維護者支援的產品。	CVE-2025-4442
D-Link	DIR-619L	1	在 D-Link DIR-619L（版本 2.04B04）中發現一個被歸類為「重大」的漏洞。此漏洞影響 `formEasySetupWizard` 函數。對引數 `curTime` 的操作會導致緩衝區溢位。攻擊可從遠端發起。供應商已在此漏洞披露初期被通知。此漏洞僅影響已不再由維護者支援的產品。	CVE-2025-4448
D-Link	DIR-619L	1	在 D-Link DIR-619L（版本 2.04B04）中發現一個漏洞，並已被歸類為「重大」。此問題影響 `formEasySetupWizard3` 函數。對引數 `wan_connected` 的操作會導致緩衝區溢位。攻擊可能從遠端發起。供應商已在此漏洞披露初期被通知。此漏洞僅影響已不再由維護者支援的產品。	CVE-2025-4449
D-Link	DIR-619L	1	D-Link 產品 DIR-619L 版本 2.04B04 存在緩衝區溢位弱點。該弱點為受影響函數 formSetEasy_Wizard 對參數 curTime 操作，會導致緩衝區溢位情況。	CVE-2025-4450
D-Link	DIR-619L	1	D-Link 產品 DIR-619L 版本 2.04B04 存在緩衝區溢位弱點。該弱點為受影響函數 formSetWAN_Wizard52 對參數 curTime 操作，會導致緩衝區溢位情況。	CVE-2025-4451
D-Link	DIR-619L	1	D-Link 產品 DIR-619L 版本 2.04B04 存在緩衝區溢位弱點。該弱點為受影響函數 formSetWizard22 對參數 curTime 操作，會導致緩衝區溢位情況。	CVE-2025-4452
Dell	Dell Storage Center - Dell Storage Manager	1	Dell 的管理模組 Dell Storage Manager 版本 20.1.20 存在驗證弱點。該弱點可能允許未經身份驗證且具有相鄰網路存取權限的攻擊者，導致權限提升情況。	CVE-2025-22477
Dell	Dell Storage Center - Dell Storage Manager	1	Dell 的管理模組 Dell Storage Manager 版本 20.1.20 存在資訊洩露弱點。該弱點為 XML 外部實體引用弱點的不當限制，導致資訊洩露情況。	CVE-2025-22478
Elastic	Kibana	1	Elastic 產品 Kibana 存在驗證弱點。攻擊者可藉由該弱點對機器學習和報告端點發送偽造 HTTP 請求，進而導致允許執行任意程式碼情況。	CVE-2025-25014

F5	BIG-IP	1	F5 產品 BIG-IP 在設備模式的 iControl REST 和 BIG-IP TMOS Shell (tmsh) 存在指令注入弱點。該弱點可能允許經過驗證的具有管理員角色權限的攻擊者執行任意系統指令。	CVE-2025-31644
F5	BIG-IP	1	F5 產品 BIG-IP 的 PEM 系統存在服務阻斷弱點。該弱點為在虛擬伺服器上啟用了 URL 分類策略或帶有 urlcat 命令的 iRule 時，未公開的請求可能會導致流量管理微內核 (TMM) 意外中止或服務阻斷情況。	CVE-2025-35995
F5	BIG-IP	1	F5 產品 BIG-IP 的 HTTP/2 httprouter 設定檔存在弱點。該弱點可能會導致記憶體資源利用率增加。	CVE-2025-36504
F5	BIG-IP	1	F5 產品 BIG-IP 的 APM 虛擬伺服器設定存在服務阻斷弱點。該弱點為使用 PingAccess 設定檔時，未公開的請求可能會導致微內核 (TMM) 意外中止或服務阻斷情況。	CVE-2025-36525
F5	BIG-IP	1	當在虛擬伺服器上設定具有強制 RFC 合規性選項的 HTTP 設定檔時，未公開的請求可能會導致流量管理微核心 (TMM) 終止。 注意：已達到技術支援結束（EoTS）的軟體版本不會進行評估。	CVE-2025-36557
F5	BIG-IP	1	當在虛擬伺服器上設定流控制傳輸協定 (SCTP) 設定檔時，未公開的請求可能會導致記憶體資源使用率增加。 注意：已達到技術支援結束（EoTS）的軟體版本不會進行評估。	CVE-2025-41399
F5	BIG-IP	1	當在虛擬伺服器上設定 HTTP/2 用戶端和伺服器設定檔時，未公開的請求可能會導致 TMM 終止。 注意：已達到技術支援結束 (EoTS) 的軟體版本不會進行評估。	CVE-2025-41414
F5	BIG-IP	1	當在虛擬伺服器上設定連線鏡像時，未公開的請求可能會導致流量管理微核心 (TMM) 在流量群組中的備用 BIG-IP 系統中終止。注意：已達到技術支援結束（EoTS）的軟體版本不會進行評估。	CVE-2025-41431
F5	BIG-IP	1	當在訊息路由虛擬伺服器上設定會話初始協定 (SIP) 訊息路由框架 (MRF) 應用層閘道器 (ALG) 設定檔時，未公開的請求可能會導致流量管理微核心 (TMM) 終止。注意：已達到技術支援結束（EoTS）的軟體版本不會進行評估。	CVE-2025-41433
F5	F5OS - Appliance	1	在 F5OS 系統上，如果 root 使用者之前已將系統配置為允許透過基於 SSH 金鑰的身份驗證登錄，然後啟用了裝置模式；仍允許透過基於 SSH 金鑰的身份驗證進行存取。攻擊者要利用此漏洞，必須取得 root 使用者的 SSH 私鑰。 注意：已達到技術支援終止（EoTS）的軟體版本不予評估。	CVE-2025-36546
F5	F5OS - Appliance	1	F5OS 上存在不當授權漏洞，遠端身分驗證使用者（LDAP、RADIUS、TACACS+）可能被授權具有更高權限的 F5OS 角色。 注意：已達到技術支援結束（EoTS）的軟體版本不會進行評估。	CVE-2025-46265

Huawei	HarmonyOS	1	文件系統模組中身份驗證邏輯實現不當的漏洞影響：成功利用此漏洞可能會影響服務機密性。	CVE-2025-46584
Huawei	HarmonyOS	1	核心模組中的越界數組讀取/寫入漏洞影響：成功利用此漏洞可能會影響可用性。	CVE-2025-46585
IBM	CICS TX Standard	1	IBM CICS TX Standard 11.1 和 IBM CICS TX Advanced 10.1 和 11.1 可允許本機使用者在系統上執行任意程式碼，因為 gethostbyaddr 函數無法處理 DNS 回傳要求。	CVE-2025-1329
IBM	CICS TX Standard	1	IBM CICS TX Standard 11.1 和 IBM CICS TX Advanced 10.1 和 11.1 可能允許本機使用者在系統上執行任意程式碼，因為無法處理 gethostbyname 函數的 DNS 回傳要求。	CVE-2025-1330
IBM	CICS TX Standard	1	IBM CICS TX Standard 11.1 和 IBM CICS TX Advanced 10.1 和 11.1 可能會因為不安全地使用 gets 函數而允許本機使用者在系統上執行任意程式碼。	CVE-2025-1331
IBM	Maximo Application Suite	1	由於基於角色的存取控制 (RBAC) 配置中的安全性設定漏洞，IBM Maximo Application Suite 9.0 可能允許具有一定存取等級的攻擊者提升其權限。	CVE-2025-2898
IBM	Sterling Partner Engagement Manager	1	IBM Sterling Partner Engagement Manager 6.1.0、6.2.0、6.2.2 JWT 機密儲存在公共 Helm Charts 中，而不是作為 Kubernetes 機密儲存。	CVE-2025-33093
IBM	Storage Scale	1	在某些設定下，IBM Storage Scale 5.2.2.0 和 5.2.2.1 可能會因輸入中和不當而允許經過驗證的使用者執行特權命令。	CVE-2025-1137
Microsoft	Azure Automation	1	Azure 自動化中的不當授權可授權攻擊者透過網路提升權限。	CVE-2025-29827
Microsoft	Azure DevOps	1	當 Visual Studio 不正確地處理管道作業令牌時，存在特權提升漏洞。成功利用此漏洞的攻擊者可以擴展其對專案的存取權限。要利用此漏洞，攻擊者首先必須訪問該項目並將短期代幣換成長期代幣。此更新透過修正 Visual Studio 更新程式處理這些令牌的方式來解決該漏洞。	CVE-2025-29813
Microsoft	Azure Storage Resource Provider (SRP)	1	Azure 中的伺服器端要求偽造 (SSRF) 允許授權攻擊者透過網路執行欺騙。	CVE-2025-29972
Microsoft	Microsoft msagsfeedbac	1	Azure 中不正確的存取控制允許未經授權的攻擊者透過網路外洩資訊。	CVE-2025-33072

	k.azurewebsites.net			
Red Hat	mirror registry for Red Hat OpenShift	1	在 Mirror Registry 中發現了一個弱點。作為 OpenShift 的 Mirror Registry 一部分提供的 quay-app 容器對 /etc/passwd 檔案具有寫入權限。此弱點允許具有該容器存取權的惡意攻擊者修改 passwd 檔案，並在該 pod 中將自身權限提升為 root 使用者。	CVE-2025-3528
Red Hat	Red Hat	1	在 Quarkus 的 quarkus-security-webauthn 模組中發現了一個弱點。Quarkus 的 WebAuthn 模組會公開預設的 REST 端點，以註冊和登入使用者，同時允許開發者提供自訂的 REST 端點。然而，即使開發者提供了自訂端點，預設端點仍然可被存取，這可能讓攻擊者獲得一個不對應任何使用者的登入 cookie，或視應用程式實作方式不同，可能對應到現有使用者，讓攻擊者僅透過知道使用者名稱就能以該使用者身分登入。	CVE-2024-12225
Tenda	AC1206	1	在 Tenda AC1206（版本最高至 15.03.06.23）中發現了一個弱點，已被列為重大弱點。此弱點影響檔案 /goform/setcfm 中的 formSetCfm 函式，參數操作會導致緩衝區溢位。此攻擊可遠端發動，且弱點細節已公開，可能被利用。	CVE-2025-4298
Tenda	AC1206	1	在 Tenda AC1206（版本最高至 15.03.06.23）中也發現了一個重大弱點。該問題影響檔案 /goform/openSchedWifi 中的 setSchedWifi 函式，操作導致緩衝區溢位。攻擊可遠端發動，弱點細節已公開，可能被利用。	CVE-2025-4299
Tenda	AC8	1	在 Tenda AC8 16.03.34.06 中發現了一個重大弱點。此弱點影響 /goform/MtuSetMacWan 檔案中的 formGetRouterStatus 函式，當參數 shareSpeed 被操作時會導致緩衝區溢位。攻擊可以遠端啟動，弱點細節已公開，可能被利用。	CVE-2025-4368
Tenda	DAP-1520	1	在 Tenda DAP-1520 1.10B04_BETA02 中發現並列為重大弱點。此弱點影響 /storage 檔案中的 check_dws_cookie 函式，操作會導致基於堆疊的緩衝區溢位。此攻擊可遠端發動，弱點細節已公開，可能被利用。	CVE-2025-4354
Tenda	DAP-1520	1	在 Tenda DAP-1520 1.10B04_BETA02 中發現了一個重大弱點，影響 /dws/api/ 中的 set_ws_action 函式。該操作會導致堆記憶體（heap）溢位。攻擊可遠端發起，弱點細節已公開，可能被利用。	CVE-2025-4355
Tenda	DAP-1520	1	在 Tenda DAP-1520 1.10B04_BETA02 中還發現了另一個重大弱點。此弱點影響 /storage 檔案中 Authentication	CVE-2025-4356

			Handler 元件的 mod_graph_auth_uri_handler 函式。操作會導致基於堆疊的緩衝區溢位，攻擊可遠端發起，弱點細節已公開，可能被利用。	
TOTOLINK	N150RT	1	在 TOTOLINK N150RT 3.4.0-B20190525 中發現了一個重大弱點。此問題涉及 /boafrm/formWsc 檔案中的未明處理程序，對 localPin 參數的操作會導致緩衝區溢位。攻擊可遠端發動，弱點細節已公開，可能被利用。	CVE-2025-4462
TOTOLINK	T10	1	在 TOTOLINK T10、A3100R、A950RG、A800R、N600R、A3000RU 和 A810R 版本 4.1.8cu.5241_B20210927 中發現了一個重大弱點。該弱點影響 /cgi-bin/cstecgi.cgi 檔案中 CloudACMunualUpdate 函式，對參數 FileName 的操作會導致緩衝區溢位。攻擊可遠端啟動，弱點細節已公開，可能被利用。	CVE-2025-4496