教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2026112309114242	發佈時間	2026-11-23 09:41:43
事故類型	ANA-漏洞預警	發現時間	2026-11-23 09:41:43
影響等級	中		

[主旨說明:]【漏洞預警】F5 NGINX 多項產品存在 5 項高風險安全漏洞(CVE-2026-113425、CVE-2026-121810、CVE-2026-123007、CVE-2026-123633 及 CVE-2026-123634)，請儘速確認並進行處置

[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-200-202611-00000019

研究人員發現 F5 NGINX Open Source、NGINX Plus 及多項內含 NGINX 之產品存在 5 項高風險安全漏洞(CVE-2026-113425、CVE-2026-121810、CVE-2026-123007、CVE-2026-123633 及 CVE-2026-123634)，類型包含使用釋放後記憶體(Use After Free)與整數下溢位(Integer Underflow)。網路上已出現 CVE-2026-123007 之概念驗證程式(PoC)，請儘速確認並進行處置。

【CVE-2026-113425】 -弱點處置期限：曝露於公眾網路＞14 天 ｜ 未曝露於公眾網路＞待下次系統更新 -評估指標結果：已知被利用[否] ｜ 被自動化利用[否] ｜ 遭利用後之影響[完全控制] 當設定為郵件代理伺服器(ngx_mail_proxy_module)時，未經身分鑑別之遠端攻擊者可透過特定流量，於 worker 處理程序觸發使用釋放後記憶體，進而造成處理程序中止或記憶體毀損而中斷服務；並可於停用或可繞過位址空間配置隨機化(ASLR)之系統上執行任意程式碼。

【CVE-2026-121810】 -弱點處置期限：曝露於公眾網路＞14 天 ｜ 未曝露於公眾網路＞待下次系統更新 -評估指標結果：已知被利用[否] ｜ 被自動化利用[否] ｜ 遭利用後之影響[完全控制] 使用 HTTP/3(ngx_http_v3_module)時，於特定情況下，未經身分鑑別之遠端攻擊者可於 worker 處理程序觸發使用釋放後記憶體，導致該處理程序重新啟動進而造成阻斷服務；並可於停用或可繞過 ASLR 之系統上執行任意程式碼。

【CVE-2026-123007】 -弱點處置期限：曝露於公眾網路＞14 天 ｜ 未曝露於公眾網路＞待下次系統更新 -評估指標結果：已知被利用[否] ｜ 被自動化利用[否] ｜ 遭利用後之影響[完全控制] 當啟用 HTTP/2(ngx_http_v2_module)時，未經身分鑑別之遠端攻擊者可傳送特定流量使流量控制視窗(flow control window)超出允許範圍，進而觸發堆積型緩衝區溢位而造成記憶體毀損，進而導致 worker 處理程序發生區段錯誤而中止；並可於停用或可繞過 ASLR 之系統上執行任意程式碼。

【CVE-2026-123633】 -弱點處置期限：曝露於公眾網路＞14 天 ｜ 未曝露於公眾網路＞待下次系統更新 -評估指標結果：已知被利用[否] ｜ 被自動化利用[否] ｜ 遭利用後之影響[完全控制] 當啟用 HTTP/2(ngx_http_v2_module)處理客戶端連線並將請求代理至後端伺服器，且 worker 處理程序之可用連線數(worker_connections)不足時，未經身分鑑別之遠端攻擊者可傳送特製請求，於 worker 處理程序觸發使用釋放後記憶體，進而造成阻斷服務；並可於停用或可繞過 ASLR 之系統上執行任意程式碼。

【CVE-2026-123634】 -弱點處置期限：曝露於公眾網路＞14 天 ｜ 未曝露於公眾網路＞待下次系統更新 -評估指標結果：已知被利用[否] ｜ 被自動化利用[否] ｜ 遭利用後之影響[完全控制] 當設定為代理伺服器且被代理之伺服器名稱含有變數，並以伺服器端內嵌(SSI)或 mirror 指令發出子請求至解析相同伺服器名稱之位置時，未經身分鑑別之遠端攻擊者可透過特製 HTTP 請求，於 worker 處理程序觸發使用釋放後記憶體，進而造成處理程序中止或記憶體毀

損；並可於停用或可繞過 ASLR 之系統上執行任意程式碼。

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:]

【F5 DoS for NGINX】4.8.0 至 4.12.0 版本

【F5 WAF for NGINX】5.9.0 至 5.16.1 版本

【NGINX App Protect DoS】4.5.0 至 4.7.0 版本

【NGINX App Protect WAF】5.4.0 至 5.8.0 版本；4.12.0 至 4.16.0 版本

【NGINX Gateway Fabric】2.0.0 至 2.8.1 版本；1.5.0 至 1.6.2 版本

【NGINX Ingress Controller】2026-lts-r1 至 2026-lts-r10 版本；5.0.0 至 5.7.1 版本；4.0.0 至 4.0.1 版本；3.7.1 至 3.7.2 版本

【NGINX Instance Manager】2.19.0 至 2.24.1 版本

【NGINX Open Source】1.31.0 至 1.31.8 版本；0.5.33 至 1.30.6 版本

【NGINX Plus】37.1.0 至 37.2.0.1 版本；37.0.0 至 37.0.7.1 版本；R34 至 R36 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://my.f5.com/manage/s/article/K000163925

https://my.f5.com/manage/s/article/K000163926

https://my.f5.com/manage/s/article/K000163927

https://my.f5.com/manage/s/article/K000163928

https://my.f5.com/manage/s/article/K000163931

https://nginx.org/en/security_advisories.html

請參考「各機關基於風險導向之弱點處置期限評估指引」，依照自身資訊資產暴露於公眾網路情形與其他評估指標，對應出弱點處置期限，並依指定期限進行處置。 網址：https://moda.gov.tw/ACS/operations/aisec/21256

[參考資料:]

1. https://nvd.nist.gov/vuln/detail/CVE-2026-113425
2. https://nvd.nist.gov/vuln/detail/CVE-2026-121810
3. https://nvd.nist.gov/vuln/detail/CVE-2026-123007
4. https://nvd.nist.gov/vuln/detail/CVE-2026-123633
5. https://nvd.nist.gov/vuln/detail/CVE-2026-123634
6. https://my.f5.com/manage/s/article/K000163925
7. https://my.f5.com/manage/s/article/K000163926
8. https://my.f5.com/manage/s/article/K000163927
9. https://my.f5.com/manage/s/article/K000163928
10. https://my.f5.com/manage/s/article/K000163931
11. https://nginx.org/en/security_advisories.html