教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2026110401111818	發佈時間	2026-11-04 13:48:19
事故類型	ANA-漏洞預警	發現時間	2026-11-04 13:48:19
影響等級	中		

[主旨說明:]【漏洞預警】Google Brotli 存在高風險安全漏洞(CVE-2026-111497)，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-200-202611-00000004

研究人員發現 Google Brotli 存在越界寫入(Out-of-Bounds Write)漏洞(CVE-2026-111497)，未經身分鑑別之遠端攻擊者可藉由特製之 Brotli 壓縮資料串流(Compressed Stream)，使解碼器記憶體寫入時超出內部緩衝區範圍，進而洩漏記憶體機敏內容、造成服務阻斷或執行任意程式碼。該漏洞已遭駭客濫用，請儘速確認並進行處置。

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:]

Google Brotli 1.0.3 至 1.0.10(不含)、1.1.0 及 1.2.0 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://github.com/google/brotli/releases/tag/v1.0.10

https://github.com/google/brotli/releases/tag/v1.1.1

https://github.com/google/brotli/releases/tag/v1.2.1

另外，有多數軟體與開發框架共用 Brotli 解壓縮元件，影響範圍涵蓋 Node.js、.NET、Python、PHP、PowerShell 及其他第三方應用程式，請確認軟體官方釋出之安全性修補或更新進行處置。

[參考資料:]

1. https://nvd.nist.gov/vuln/detail/CVE-2026-111497
2. https://github.com/google/brotli/releases/tag/v1.0.10
3. https://github.com/google/brotli/releases/tag/v1.1.1
4. https://github.com/google/brotli/releases/tag/v1.2.1