

全方位漏洞情資：修補緩解一次到位

漏洞管理的三大挑戰

在漏洞因應和管理上，現代組織大多面臨三大挑戰：漏洞數量暴增難以掌握、來源雜訊過多且難以過濾、修補優先順序難以判斷。這些問題讓資安人員無法有效識別真正具風險的漏洞，也無法在有限資源下妥善排序處理。ThreatVision 提供經專家篩選與持續更新的漏洞情資，搭配可行修補與緩解建議，協助組織聚焦處理高風險漏洞，建立更有系統、更具效率的漏洞管理流程。

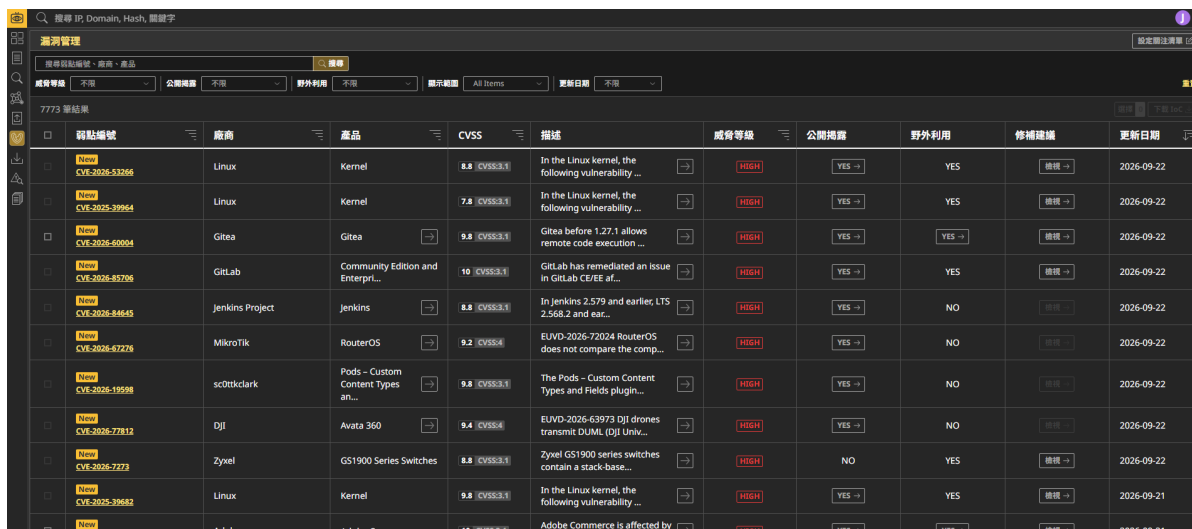
深度廣度兼具的關鍵漏洞資訊

漏洞情資暨應對緩解雙週報 (Vulnerability Insights Report, 又稱 VIR)

VIR 由 TeamT5 資深分析師團隊撰寫，聚焦近期遭大規模利用的高風險漏洞，說明其實際攻擊情境、涉入攻擊族群與受影響產業，協助使用者評估漏洞的風險與攻擊關聯性。報告內容涵蓋 CVE 編號、CVSS 分數與技術細節，協助組織即時因應並降低潛在風險；同時提供緩解策略與偵測工具，使組織在無法立即修補時，也有對策。VIR 每兩週更新一次，全年共提供 24 份報告。

漏洞修補管理情資模組 (Patch Management)

漏洞管理持續更新並彙整高風險漏洞關鍵資訊，由 TeamT5 威脅狩獵研究團隊透過風險評估模型，交叉比對多個具公信力的情資來源，篩選出已公開揭露、遭野外利用或已有可用利用工具的高風險漏洞，並提供受影響產品、修補資訊與公開可取得的概念驗證程式碼（PoC）等重要資訊，協助評估風險與排定修補優先順序。除了已知漏洞，團隊同時主動追蹤零日漏洞，以利使用者及早掌握風險並規劃主動防禦策略。



漏洞編號	廠商	產品	CVSS	描述	威脅等級	公開揭露	野外利用	修補建議	更新日期
CVE-2025-53266	Linux	Kernel	8.8 [CVSS:3.1]	In the Linux kernel, the following vulnerability ...	HIGH	YES →	YES	修補 →	2025-09-22
CVE-2025-39964	Linux	Kernel	7.8 [CVSS:3.1]	In the Linux kernel, the following vulnerability ...	HIGH	YES →	YES	修補 →	2025-09-22
CVE-2025-60004	Gitea	Gitea	9.8 [CVSS:3.1]	Gitea before 1.27.1 allows remote code execution ...	HIGH	YES →	YES →	修補 →	2025-09-22
CVE-2025-85706	GitLab	Community Edition and Enterprise	10 [CVSS:3.1]	GitLab has remediated an issue in GitLab CE/EE af...	HIGH	YES →	YES	修補 →	2025-09-22
CVE-2025-84645	Jenkins Project	Jenkins	8.8 [CVSS:3.1]	In Jenkins 2.579 and earlier LTS 2.568.2 and ear...	HIGH	YES →	NO	修補 →	2025-09-22
CVE-2025-63276	Mikrotik	RouterOS	9.2 [CVSS:3.1]	EUVN-2025-72024 RouterOS does not compare the comp...	HIGH	YES →	NO	修補 →	2025-09-22
CVE-2025-19598	sc0ttkclark	Pods - Custom Content Types and Fields plugin...	9.8 [CVSS:3.1]	The Pods - Custom Content Types and Fields plugin...	HIGH	YES →	NO	修補 →	2025-09-22
CVE-2025-77812	DJI	Avata 360	9.4 [CVSS:3.1]	EUVN-2025-63973 DJI drones transmit DUMIL (DJI Univ...	HIGH	YES →	NO	修補 →	2025-09-22
CVE-2025-7273	Zyxel	GS1900 Series Switches	8.8 [CVSS:3.1]	Zyxel GS1900 series switches contain a stack-base...	HIGH	NO	YES	修補 →	2025-09-22
CVE-2025-39682	Linux	Kernel	9.8 [CVSS:3.1]	In the Linux kernel, the following vulnerability ...	HIGH	YES →	YES	修補 →	2025-09-21
CVE-2025-39682	Adobe	Adobe Commerce	10 [CVSS:3.1]	Adobe Commerce is affected by	HIGH	YES →	YES →	修補 →	2025-09-21

針對漏洞的威脅狩獵工具

TeamT5 的威脅狩獵工具由資深分析師團隊自主開發，可檢測 VIR 中提到的漏洞。團隊採用多項易於應用的工具，例如 YARA、Snort 和 Sigma 規則，以及各種腳本。這些工具可在用戶端裝置上執行，有效檢測漏洞並快速識別被利用情況，提升整體偵測與回應效率。

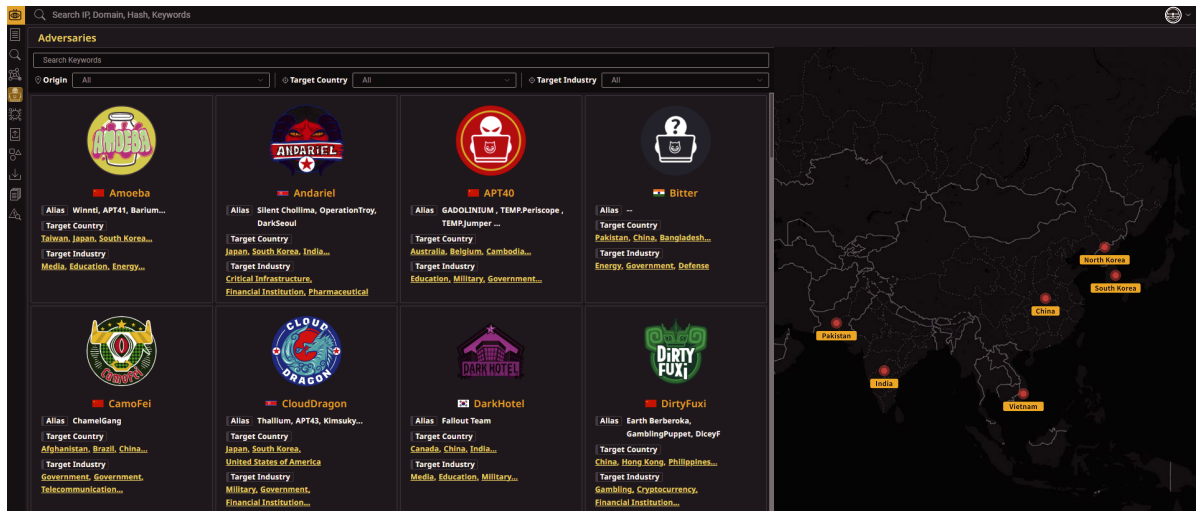
漏洞情資暨應對緩解雙週報	漏洞修補管理情資模組
• 提供高風險漏洞的深入分析 • 說明攻擊情境並提供緩解方法 • 提供緩解方案與 TeamT5 獨家偵測工具 • 可減少高風險漏洞所造成的威脅 • 每兩週 1 份，每年 24 份 • 提供英文版	• 優先聚焦經專家驗證與篩選的高風險漏洞 • 掌握漏洞公開揭露與野外利用狀況 • 依受影響產品資訊評估衝擊範圍 • 運用修補資訊與公開 PoC 協助漏洞處置 • 及早掌握零日漏洞風險

ThreatVision 漏洞解析 + 修補管理：因應漏洞最佳解方



ThreatVision 平台一覽

多元情資支援不同角色與任務，協助組織全面掌握攻擊族群的行為模式、預先部署防禦策略，是從資安戰略規劃到第一線防禦的最佳助力。



如何開始使用 ThreatVision

請聯繫 TeamT5 業務並申請 14 天的 ThreatVision 試用帳戶。如果希望了解產品相關的進一步資訊，請發送電子郵件至 sales@teamt5.org。我們期待與您合作，協助您的組織免受網路威脅。

關於 TeamT5

v.202609

廣受全球 550 家以上客戶信賴，橫跨政府單位、科技、製造、金融、醫療、軍事、電信等產業。

頂尖專家團隊

團隊成員常在世界級資安會議中發表最新頂尖研究，包含臺灣 HITCON、美國 Black Hat、日本 Code Blue / AVTOKYO、德國 Troopers，及國際組織辦理的 Hack In The Box 與 FIRST，於威脅情資研究與資安先進技術領域擁有世界領先地位。

外界肯定

獲得美國 Bloomberg 及 CNN、日本產經新聞及朝日新聞、韓國 ET News 等採訪報導。更於 2022 年獲得日本三大巨頭投資，包含日本最大創投 JAFCO 集富集團、日本最大跨國企業並在全球皆有商業投資的 ITOCHU 伊藤忠商事，與日本最大資安解決方案提供商 MACNICA。