運用 Cisco Talos 智慧 讓資安弱點無所遁形

資料提供者：思科台灣首席資安顧問 游証硯

回首 2020 年，若從資訊安全角度來看，堪稱得上是動盪之年。尤其以層出不窮的勒索病毒攻擊事件、導致眾多知名大型企業或機構遭駭，最讓人觸目驚心，據資安業者統計，2020 年第三季平均每天的勒索軟體攻擊行動次數，比當年上半年大增 50%，平均每 10 秒就出現一個新的受害者。

前述資安威脅之所以越演越烈，與疫情衍生的遠距工作新常態，有著密切關聯。隨著越來越多員工以家庭，甚或連鎖咖啡廳、速食店為工作場域，經由各式各樣的個人裝置存取企業網路，這些連線行為皆已脫離企業安全堡壘的範圍，給予駭客可乘之機。儘管企業因此而面臨莫大資安風險，但 Cisco Talos 系統弱點研究團隊調查分析發現，只要確實做好漏洞揭露和修補，就足以防止許多攻擊。

光 2020 年，Cisco Talos 系統弱點研究團隊從範圍廣泛的產品項目之中，共計發現了 231 個弱點，這些弱點皆已獲得修補與發佈，大大減少駭客發動攻擊的機會。Talos 團隊有鑑於疫情遲未消退、遠距工作模式依然盛行，所以在 2020 年特別針對程式碼、Web ／行動設備及驅動程式弱點加強分析。在接下來的文章篇幅中，將述說該團隊在 2020 年締造的弱點分析成果。

弱點分析原則

Cisco Talos 系統漏洞研究團隊調查分析的範疇，主要涵蓋軟體、作業系統、物聯網裝置、應用服務、Web 與行動設備，目的在於保護思科的客戶，以及眾多的網路服務及網路社群。

Talos 透過一項為期 90 天的基本時間表，來定義、協調、分析與揭露其所發現到的漏洞。在將近三個月的期程中，Talos 與相關供應商（Vendor）展開合作，確保能及時產生修補程式和緩解策略，進而化解掉這些可能被駭客利用的攻擊媒介；而 Talos 提出的檢測內容，可以協助供應商在應變期間內妥善保護客戶。另值得一提，Talos 也同時對外公開檢測內容和詳細報告，讓客戶可以從 Talos 網站 https://talosintelligence.com/vulnerability_info 中，找到需要高度關注的系統弱點資訊。

不僅如此，Talos 還會定期發佈 Vulnerability Spotlight 部落格文章，針對發現到的系統弱點進行深入的技術剖析，並簡單扼要地述說各個弱點可能造成的影響。客戶可透過相關網站 https://blog.talosintelligence.com/ 找尋到這些 Spotlight 部落格文章。

依據思科的供應商系統弱點與揭露政策，Talos 制定了以下的作業時間表：

- Day 0：1. 與供應商初次聯繫。
  2. 向思科客戶發佈如何利用思科安全產品啟動保護措施。
  3. 假使供應商並非 CNA（CVE 編號管理者），則進行 CVE（公開弱點與揭露）配置。
  4. 與此同時，Cisco Talos 漏洞追蹤網站將列出相關供應商名稱與報告日期。
- Day 7：如果供應商未提出回應，Talos 將展開第二次聯繫。
- Day 45：向供應商發出電子郵件提醒，其中包含漏洞報告的發佈日期。
- Day 60：若供應商未回應或已停止回應，則發送最終電子郵件提醒。
- Day 90：在 Cisco Talos 漏洞追蹤網站上揭露完整的漏洞報告；但如果供應商在第 90 天前發佈該漏洞的修補程式或緩解措施，則思科將在供應商發佈後就會立即揭露完整的漏洞報告，並向 MITRE 提交 CVE 發佈請求。

綜觀 2020 年 Talos 發佈的 231 份分析報告，一共涉及 277 個 CVE，範圍涵蓋作業系統、IoT 設備、Microsoft Office 產品、瀏覽器、PDF 閱讀器等；值得留意的是，從 2019 年起，Talos 的檢測、分析及調查工作中涉及到的 CVE 數量，都明顯較前一年大幅增加，代表系統漏洞數量快速攀升中。

儘管眾家供應商努力增加技術覆蓋範圍，積極提升 Internet 整體安全性，但至今仍未出現 100% 絕對安全的軟體，即使擁有大型資安團隊的供應商也難免犯下若干錯誤。Cisco Talos 致力於在不安全的軟體與硬體環境中、持續擴大對系統弱點的檢測覆蓋範圍，其初衷並非對任何一家供應商提出技術挑戰，而是喚起大家重視安全編碼、安全開發，盡量避免為駭客製造趁隙而入的機會。

2020 年 Talos 發現哪些弱點？

1. PDF 應用程序（包括 Adobe PDF，Foxit PDF，NitroPDF 和 Google PDFium）中存在多項弱點。
2. Intel、NVIDIA 和 AMD 的圖形驅動程式中存在多個弱點，導致微軟決定於 2021 年二月以前，在 Windows 中完全停用 RemoteFX vGPU 功能。
3. Pixar OpenUSD 存在多項弱點。
4. Talos 參與 Microsoft Azure Sphere 研究挑戰的過程中，在 Azure Sphere 中發現另外 16 個弱點。
5. Firefox、Chrome 和 Safari 等主要 Web 瀏覽器中存在多個弱點，包括許多瀏覽器皆採用的 WebKit 系統。
6. 包括 Synology 的 SRM 與 DSM 韌體，以及 Microsoft Office、Windows 等其他主要應用程式，都被發掘出弱點。

Talos 根據一致的揭露政策，與所有供應商緊密合作，確保在修正檔發佈以前，思科的客戶及網路社群都能受到適當的保護。由此可見，這項富含前瞻性的研究計畫可謂意義重大，足以催生更安全的軟體與硬體，令全球所有網路使用者共同受益。

關於 Talos 揭露的弱點，請參考 Talos 的弱點報告網站：
http://www.talosintelligence.com/vulnerability_reports/

想瞭解 Talos 的弱點揭露政策，可參考以下網站：
https://tools.cisco.com/security/center/resources/vendor_vulnerability_policy.html

本文資料料來源：https://blog.talosintelligence.com/2020/12/vulnerability-discovery-2020.html

更多資訊請參考聚碩官網 www.sysage.com.tw