張貼日期：2023/10/16

【漏洞預警】HTTP2 協定漏洞放大攻擊，多家業者統計最大DDoS攻擊流量皆創紀錄。

- 主旨說明：【HTTP2 協定漏洞放大攻擊，多家業者統計最大DDoS攻擊流量皆創紀錄。
- 內容說明：
  - 轉發 CHTSECURITY-200-202310-00000002】
  - Google、Cloudflare與 Amazon Web Services（AWS）本周二（10/10）分別公布了涉及 HTTP/2 協定的 CVE-2023-44487 零時差安全漏洞，原因是它們在今年的8月至10月間，全都面臨了肇因於該漏洞的分散式服務阻斷（DDoS）攻擊，且其攻擊規模對上述業者來說皆為史上最大，例如 Google 所緩解的攻擊流量達到每秒3.98億次的請求，是Google 上一個紀錄的7.5倍。
  - HTTP/2 標準在2015年出爐，最新的則是2022年6月頒布的 HTTP/3。不過，根據 Cloudflare 截至今年4月的統計，目前最普及的協定仍是HTTP/2，市占率超過60% 存在於 HTTP/2 中的 CVE-2023-44487 漏洞可導致快速重置攻擊，它利用 HTTP/2 中的多工串流 (Stream Multiplexing) 功能，發送大量的請求且立即取消，因而造成伺服器端的大量工作負載，卻只需要少量的攻擊成本。
  - HiNet SOC 建議管理者儘速評估並修補漏洞更新，以降低受駭風險。
- 影響平台:
  - 具 HTTP/2 協定傳輸的應用軟體或服務
- 建議措施:
  - 具 HTTP2 協定支援多工串流 (Stream Multiplexing) 的應用軟體或服務會受影響，建議支援 HTTP2 的各家提供的說明進行修補 CVE-2023-44487漏洞，或可參考微軟公布了針對該漏洞的應對措施。
- 參考資料:
  1. iThome：https://www.ithome.com.tw/news/159221
  2. Microsoft：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-44487
  3. Google：https://cloud.google.com/blog/products/identity-security/google-cloud-mitigated-largest-ddos-attack-peaking-above-398-million-rps
  4. Cloudflare：https://blog.cloudflare.com/technical-breakdown-http2-rapid-reset-ddos-attack/

計算機與通訊中心
網路系統組 敬啟