DNS Cache Poisoning Attack Notes

美國加州大學與中國北京清大的資安專家，日前聯合發表研究報告；研究人員發現一種新式攻擊手法，可利用 Linux 存在的弱點發動 DNS 快取污染攻擊[[1]](#footnote-1)。  
  
DNS 快取污染攻擊係透過大量發送偽造的 DNS 查詢交易 ID，來將受害者的網路連線導向至偽造的網站伺服器；一般認為已於 2008 年透過隨機連接埠技術解決，也就是 DNS 查詢接收使用的連接埠不再固定使用 port 53，而會隨機使用 port 0 到 port 65535。即使攻擊者猜中了查詢者使用的交易 ID，也很難猜中查詢封包使用哪一個連接埠來傳送。  
  
隨機連接埠技術看似解決了 DNS 快取污染的問題，但兩所大學的研究人員近來發現，可以利用「旁路攻擊」的技術來找出 DNS 用戶端查詢時使用的連接埠，從而使隨機連接埠的防護技術失效。  
  
研究報告指出，由於 Linux 核心在處理 ICMP 查詢時，雖然會限制每個用戶1秒只能查詢1000次，但這個限制只針對單一用戶端使用的連接埠；換言之，攻擊者可以同時利用1000個不同的連接埠來發送 DNS 查詢要求，就能根據 Server 的回應，找出可供使用的連接埠號，從而大大提高猜中 DNS 查詢使用連接埠號的機率，進而發動 DNS 快取污染攻擊。  
  
Linux 的這個漏洞已在日前編為 CVE-2020-25705[[2]](#footnote-2)，其 CVSS[[3]](#footnote-3) 危險程度評分達 7.3 分；已在 5.10 版的 Linux 核心版本中得到修補。

Linux弱點導致 DNS 緩存中毒攻擊回歸

北京清華和加州大學的研究人員發現一種DNS 緩存中毒攻擊的新方法。這一新發現重振了 2008 年的一個錯誤，該錯誤曾被認為已經徹底解決。

什麼是 DNS 欺騙或緩存中毒?

域名系統 (DNS) 最好理解為互聯網的電話簿。

就像，當你想給你的朋友亞歷克斯打電話時，你需要通過一個叫做電話簿的系統來查找他們的電話號碼。

同樣，當您瀏覽到某個域時，您的 Web 瀏覽器會嘗試通過稱為 DNS 的 Internet 目錄系統查找它來識別其 IP 地址。

實際過程發生在一系列步驟中，並不總是那麼簡單。

例如，如果您或您網絡上的某個人之前訪問過 bleepingcomputer.com，我們的 IP 地址將被緩存在您計算機的某個地方或中間服務器上。

這意味著下次您訪問 bleepingcomputer.com 時，無需再次進行 DNS 查找。您的計算機或網絡瀏覽器已經知道在哪裡可以找到我們。

DNS緩存中毒攻擊是指污染中間服務器上存在的緩存。

想像一下，如果您的計算機（客戶端）一直依賴的 DNS 緩存來查找 bleepingcomputer.com 的 IP，返回給您的 IP 地址不正確，而不是我們的？

如果攻擊者能夠毒害 DNS 緩存，他們可能會在互聯網上造成嚴重破壞。

安全研究員 Dan Kaminsky 在 2008 年發現了這樣一個漏洞。

當設備使用 DNS 查找域名的 IP 地址時，它會在對 DNS 服務器的請求中包含一個唯一的“事務 ID”號。

當服務器以一個答案響應設備時（例如，可以在 104.20.60.209 找到 bleepingcomputer.com），設備將僅接受該響應為有效，如果它還包含該原始交易 ID。

這樣做的原因很簡單：防止流氓 DNS 服務器向您的設備充斥惡意、無效的 DNS 條目。

如果這些檢查沒有到位，流氓 DNS 服務器很容易給用戶一個欺騙的 IP 地址，當連接到一個網站時，用戶現在會被重定向到攻擊者的服務器而不是合法的服務器——感謝欺騙DNS 響應。

然而，Kaminsky 發現只有 65,536 個可能的交易 ID。

因此，攻擊者可以發送多個 ID 為 0 到 65,535 的虛假 DNS 響應，同時阻止第一個響應被緩存。

為了防止緩存第一個 DNS 響應，攻擊者會發送帶有輕微變化的域的響應，例如每個響應都包含不同的子域：1.bleepingcomputer.com、2.bleepingcomputer.com 等等。

最終，攻擊者將能夠猜測 DNS 請求的正確事務 ID，並同時通過 DNS 響應提供他們的惡意服務器 IP。

下一次，用戶訪問 bleepingcomputer.com，如果此類攻擊成功，該域將解析到攻擊者的服務器。

DNS緩存中毒是如何返回的？

為防止 DNS 緩存中毒攻擊，已實施源端口隨機化。

這意味著，即使作為攻擊者，即使我最終可以猜到您的設備在 DNS 請求中指定的 65,536 個事務 ID 之一，我也不知道將 DNS 響應發送到哪裡——因為現在您的設備正在執行 DNS 查找所以從一個隨機端口（理論上也有 65,536 個值）而不是端口 53。

考慮到數十億種可能性，這種解決方案使 DNS 緩存中毒攻擊幾乎不可能通過 Kaminsky 發現的方法進行。

但清華大學和加州大學的研究人員發布了一種利用側信道攻擊來推斷 DNS 客戶端源端口號的方法。

隨著源端口被排除在外，通過如上所述的猜測事務 ID 再次可以進行 Kaminsky 的 DNS 緩存中毒攻擊。

由於 Linux 內核如何處理 ICMP 請求（想想 ping 或 tracert），因此猜測源端口成為可能。

為了節省帶寬，Linux 內置的速率限制器將傳入請求的數量默認為每秒 1,000 個，並使用計數器來跟踪這些請求。

對於在基於 Linux 的服務器上的關閉端口收到的每個請求，計數器將減 1，服務器將響應“無法訪問”。

這意味著，在一秒鐘內，如果您向服務器上的不同隨機端口發送 1,000 個數據包，所有這些端口都已關閉，那麼服務器會在那一秒內切斷您的連接。

但是，這也會告訴您，您對哪個端口可以打開的所有 1,000 次猜測都是錯誤的。

有趣的是，對於在有效的開放端口接收到的每個請求，計數器都不會遞減。而且，服務器顯然不會發送“無法訪問”。

這意味著，每一秒，攻擊者都可以用 1,000 個發往隨機端口的欺騙性數據包淹沒 DNS 解析器。

以這種方式，在幾秒鐘內，攻擊者將能夠推斷出他們試圖毒化的 DNS 解析器上所有打開的端口。

有了正確端口的知識，他們就可以重新利用 Kaminsky 的漏洞來引發 DNS 中毒攻擊。

影響多個 DNS 解析（例如 BIND、Unbound、dnsmasq）的 2020 年 DNS 緩存中毒漏洞已被暱稱為 SAD DNS（Side-channel AttackeD DNS）並分配了 CVE-2020-25705。

那麼有沒有解決辦法呢？

就像源端口隨機化為攻擊者增加了一些複雜性一樣，Linux 內核隨機化速率限制器的最大值而不是始終使用 1,000 可能證明是有用的。

這樣的修復將使攻擊者再次難以推斷出正確的端口以針對 DNS 欺騙攻擊。

BlueCat 的軟件安全總監 David Maxwell 提出了一個建議：

“Linux 引入的自動隨機化 ratelimit 值的更改已於 10 月 16 日包含在 Linux 內核中，這意味著大多數係統還需要一段時間才能運行它。它還沒有發布。與此同時，你可以使用"因此，我們目前正在努力為社區提供類似的示例腳本。”

對 Linux 內核的 icmp.c 文件所做的修復現在為計數器分配了一個隨機值（稱為“信用”），但正如 Maxwell 解釋的那樣，世界各地的 Linux 服務器可能需要一段時間才能趕上。

研究人員提出的其他解決方案包括通過禁用傳出 ICMP 或隨機化速率限制值（如 Linux 開發人員所做的那樣）來破壞側信道本身，減少 DNS 查詢超時以最小化攻擊窗口，以及使用 DNSSEC 等技術、DNS cookie 或 0x20 位編碼以向 DNS 消息添加機密。

但是，Maxwell 不建議完全阻止 ICMP 流量，因為該協議具有合法的用例，例如在 IPv6 分片中。

“如果 DNS 服務器完全阻止了 ICMP，則區域傳輸可能會失敗，如果在它和另一台服務器之間存在一個 MTU 較小的躍點（阻止 ICMP 會導致 PMTUD 黑洞），”Maxwell 告訴 BleepingComputer。

這種旁道攻擊的發現給互聯網工程師帶來了額外的壓力，要求他們加強 DNS 安全性。

DNS 已經是一種相對不安全的協議，旨在提高速度而不是性能和安全性。

即使構建諸如 DNS-over-HTTPS (DoH) 之類的增強功能也無法阻止攻擊者濫用 DNS 進行惡意活動。

2020 年 11 月 13 日更新：已添加，此漏洞被跟踪為 CVE-2020-25705。添加了研究人員提出的解決方案。

此外，據研究人員稱，該漏洞還會影響如下所示尚未發布補丁的其他操作系統。

“除了 Linux，我們已經證實其他主要操作系統內核也容易受到攻擊，儘管全球速率限制較低——Windows 和 FreeBSD 為 200，MacOS 為 250，”研究人員在他們的論文中表示。

Linux 3.18-5.10

Windows Server 2019（版本 1809）和更新版本（我們沒有測試舊版本）

macOS 10.15 及更高版本（我們沒有測試舊版本）

FreeBSD 12.1.0 和更新版本（我們沒有測試舊版本）

Linux 的補丁已集成到 5.10 中並向後移植到許多穩定版本。但是，我們不知道 Windows/macOS/FreeBSD 將如何以及何時修補此漏洞。

1. https://www.twcert.org.tw/tw/cp-104-4146-0ab45-1.html [↑](#footnote-ref-1)
2. CVE-2020-25705 (<https://access.redhat.com/security/cve/cve-2020-25705>) - A flaw in the way reply ICMP packets are limited in the Linux kernel functionality was found that allows to quickly scan open UDP ports. This flaw allows an off-path remote user to effectively bypassing source port UDP randomization. The highest threat from this vulnerability is to confidentiality and possibly integrity, because software that relies on UDP source port randomization are indirectly affected as well. [↑](#footnote-ref-2)
3. 這個漏洞有多嚴重? (<https://ithelp.ithome.com.tw/articles/10203313>) [↑](#footnote-ref-3)