ASA BEAST漏洞解決方案

目錄

簡介

本文檔介紹思科自適應安全裝置(ASA)軟體中存在允許未經授權的使用者訪問受保護內容的漏洞。還介紹了此問題的解決方法。

問題

攻擊者利用Browser Exploit Against SSL/TLS(BEAST)漏洞，以已知明文攻擊方式通過密碼塊鏈接(CBC)加密模式中的初始化向量(Initialization Vector,IV)連結有效讀取受保護的內容。

該攻擊使用一種工具，該工具利用廣泛使用的傳輸層安全第1版(TLSv1)協定中的漏洞。問題不在於協定本身，而在於協定使用的密碼套件。TLSv1和安全套接字層第3版(SSLv3)青睞CBC密碼，即發生填充Oracle攻擊。

使用者影響

根據Trustworthy Internet Movement建立的SSL Pulse SSL實施調查，75%以上的SSL伺服器容易受到此漏洞的攻擊。但是，BEAST工具所涉及的後勤工作相當複雜。為了使用BEAST竊聽流量，攻擊者必須能夠非常快速地讀取和注入資料包。這可能限制了BEAST攻擊的有效目標。例如，BEAST攻擊者可以有效地在WIFI熱點或所有Internet流量都通過有限數量的網路網關進行封鎖時獲取隨機流量。

解決方案

BEAST是協定使用的密碼弱點的一種攻擊方式。由於此問題會影響CBC密碼，因此最初解決方法是切換到RC4密碼。然而,2013年發表的RC4文章的關鍵排程演算法的弱點揭示出，即使RC4也存在使其不合適的弱點。

為了解決此問題，Cisco為ASA實施了以下兩個修復：

- 思科錯誤ID CSCts83720:*升級到TLS 1.1/1.2*

升級並使用TLS 1.1/1.2。此解決方案的侷限性是它僅適用於ASA 5500-X ASA平台。傳統ASA平台（ASA 5505和ASA 5500系列）上的加密硬體不支援TLSv1.2。因此，無法修復這些平台。

由於通訊協定限制，沒有適用於SSLv3或TLSv1.0的解決方案；但是，大多數現代瀏覽器都實施了不同的緩解方法。

- 思科錯誤ID CSCuc85781:*WebVPN Cookie隨機化*

對於不支援TLSv1.2的ASA軟體版本，思科通過此修復將cookie隨機化，以降低風險。這並不能完全阻止BEAST攻擊，但有助於緩解這些攻擊。

提示：完全避免BEAST漏洞的唯一方法是使用TLSv1.2。這類似於密碼。思科不斷在更新的代碼中新增更新、更強大的密碼，而較舊的密碼可能存在已知問題（例如RC4）。 因此，思科建議您使用較新的協定和密碼。