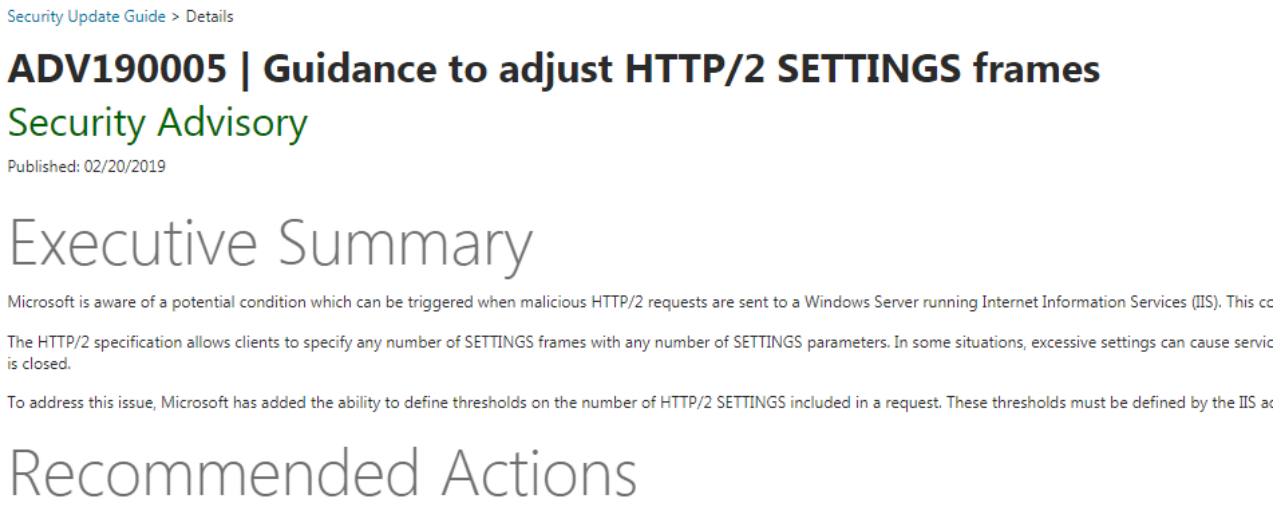
微軟修補 IIS 造成 CPU 使用率飆到 100%的漏洞

微軟公開一個存在於 IIS 的漏洞，能讓駭客進行阻斷服務（DoS）攻擊癱瘓網站，呼籲 IIS 管理員最好儘速安裝修補程式

文/林妍溱 | 2019-02-22 發表


Security Update Guide > Details

ADV190005 | Guidance to adjust HTTP/2 SETTINGS frames

Security Advisory

Published: 02/20/2019

Executive Summary

Microsoft is aware of a potential condition which can be triggered when malicious HTTP/2 requests are sent to a Windows Server running Internet Information Services (IIS). This cc

The HTTP/2 specification allows clients to specify any number of SETTINGS frames with any number of SETTINGS parameters. In some situations, excessive settings can cause servic is closed.

To address this issue, Microsoft has added the ability to define thresholds on the number of HTTP/2 SETTINGS included in a request. These thresholds must be defined by the IIS ac

Recommended Actions

微軟 2 月 20 日發出安全公告，警告一隻存在 IIS 中的漏洞可能讓駭客發動惡意 HTTP/2 呼叫，讓系統 CPU 使用率衝高到 100%，藉此發動阻斷服務（denial of service, DoS）攻擊，令網站斷線。

HTTP/2 是 1999 年釋出的 HTTP/1.1 之後的更新版，大幅改善了瀏覽器的網頁下載速度。根據微軟 ADV190005 的安全公告，HTTP/2

規格能讓用戶端指定 SETTINGS frames 的任何參數。但在某些情況下，過度設定可能使網頁服務不穩定，導致伺服器 CPU 使用量短時間衝高到 100%，一直到達連線時間上限，由網頁伺服器 IIS 切斷連線，也就達到了 DoS 攻擊的效果。

受到本漏洞影響的產品包括 Windows 10 及 Windows Server 2016 中的 IIS。

為解決上述漏洞，微軟已釋出非安全累積更新，包括 KB4487006、KB4487011KB4487021 及 KB4487029。在這些修補程式中，微軟為 IIS 加入為 HTTP/2 呼叫定義 SETTINGS 數量閥值的功能。這個閥值必須由 IIS 管理員定義，而非由微軟預設。至於要怎麼定義，微軟也公佈相關的支援說明。

微軟表示本漏洞沒有緩和威脅或權宜作法，呼籲 IIS 管理員最好儘速安裝修補程式。

資料來源：iThome