行政院國家資通安全會報技術服務中心

漏洞/資安訊息警訊

發布編號	NCCST-ANA-2016-0094	發布時間	Fri Sep 30 09:39:35 CST 2016
事件類型	漏洞預警	發現時間	Sat Sep 24 00:00:00 CST 2016
警訊名稱	Cisco IOS 系列軟體與 PIX 防火牆存在零時差漏洞(CVE-2016-6415)，允許攻擊者遠端獲取記憶體內容，導致機敏資訊外洩		
內容說明	美國思科(Cisco)公司今年 8 月得知國際名為影子掮客(The Shadow Brokers)駭客團體所釋出的網路攻擊工具後，開始調查相關攻擊工具所利用的安全漏洞，於 2016 年 9 月 16 日公布發現一個波及 Cisco IOS、Cisco IOS XE、Cisco IOS XR 軟體及 Cisco PIX 防火牆的零時差漏洞(CVE-2016-6415)。 該漏洞主要是因為 Cisco IOS、Cisco IOS XE、Cisco IOS XR 軟體及 Cisco PIX 防火牆中，負責處理網路密鑰交換(Internet Key Exchange version 1，IKEv1)協商請求(Negotiation Requests)的程式碼未能充分的進行條件檢查，因此當遠端攻擊者發送一個惡意的 IEKv1 封包到可接受 IEKv1 協商請求的裝置上，便能獲取記憶體內容，進而導致裝置上的機敏資訊外洩。		
影響平台	1.Cisco PIX Firewall： -5.2(9)至 6.3(4)(含)版 2.Cisco IOS： -12.2 至 12.4(含)版 -15.0 至 15.6(含)版 3.Cisco IOS XE： -3.1S 版 -3.2S 版 -3.3S 版、3.3SG 版、3.3XO 版		

	-3.4S 版、3.4SG 版 -3.5E 版、3.5S 版 -3.6E 版、3.6S 版 -3.7E 版、3.7S 版 -3.8E 版、3.8S 版 -3.9E 版、3.9S 版 -3.12S 至 3.18S(含)版 -16.1 至 16.3(含)版 4.Cisco IOS XR： -所有 4.3.x(含)版 -所有 5.0.x(含)版 -所有 5.1.x(含)版 -所有 5.2.x(含)版
影響等級	高
建議措施	請各機關可聯絡設備維護廠商或利用「show version」指令確認當前使用的軟體版本，若版本為受影響之 Cisco IOS、Cisco IOS XE、Cisco IOS XR 軟體版本，則請參考以下建議資訊： 1. 目前因 Cisco 官方尚未針對 Cisco IOS、Cisco IOS XE、Cisco IOS XR 釋出修復版本，所以仍請密切注意 Cisco 官方網頁(https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160916-ikev1)之更新訊息。 2. 使用 Cisco 官方網頁(https://tools.cisco.com/security/center/viewIpsSignature.x?signatureId=7699&signatureSubId=0&softwareVersion=6.0&releaseVersion=S942)所提供的入侵防禦系統(IPS)特徵檔 7699-0，或 Sourcefire 官方網頁(https://support.sourcefire.com/supplemental/sf-rules-2016-09-16-seu.html)所提供的 Snort 入侵規則檔 SID 40220(1)、SID 40221(1)、SID 40222(1)，以協助偵測與阻止嘗試利用此漏洞之攻擊。

	其它事項： Cisco PIX Firewalls 設備，因產品過舊，目前已無相關的修復程式。
參考資料	1.http://www.ithome.com.tw/news/108639 2.http://www.securityfocus.com/bid/93003 3.http://thehackernews.com/2016/09/cisco-nsa-exploit.html 4.https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-6415 5.https://tools.cisco.com/security/center/selectIOSVersion.x

此類通告發送對象為通報應變網站登記之資安人員。若貴 單位之資安人員有變更，可逕自登入通報應變網站（https://www.ncert.nat.gov.tw）進行修改。若您仍為貴單位之資安人員但非本事件之處理人員，請協助將此通告告知相關處理人員。

如果您對此通告的內容有疑問或有關於此事件的建議，請勿直接回覆此信件，請以下述聯絡資訊與我們連絡。

地 址： 台北市富陽街 116 號
聯絡電話： 02-27339922
傳真電話： 02-27331655
電子郵件信箱： service@nccst.nat.gov.tw