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-2016-0121	發布時間	Fri Nov 25 10:12:09 CST 2016
事件類型	漏洞預警	發現時間	Thu Nov 17 00:00:00 CST 2016
警訊名稱	部分網路設備存在對於網路控制訊息協定（ICMP）封包處理之弱點，使得攻擊者可藉由持續傳送「無法到達目的地且無法存取傳輸埠」的 ICMP 封包，造成網路設備癱瘓，進而導致服務中斷		
內容說明	2016 年 11 月 8 日，丹麥的資安業者 TDC Security Operations Center 公開一項名為黑護士(BlackNurse)的網路攻擊手法，根據報告指出，該攻擊只需透過少量「無法到達目的地且無法存取傳輸埠」（ICMP Type 3 Code 3）之 ICMP 封包，即可造成部分防火牆或網路設備 CPU 過載，持續攻擊將造成服務中斷，導致內部使用者無法存取外部網路。		
影響平台	目前已知受影響的網路設備廠牌與型號如下： 1.Cisco ASA 5505、5506、5515、5525 及 5540 2.Cisco 6500 routers with SUP2T 與 Netflow v9 on the inbound interface 3.Cisco ASA 5550 與 5515 各系列 4.Cisco Router 897 5.SonicWall 6.Palo Alto 5050 7.Zyxel NWA3560-N 8.Zyxel Zywall USG50 9.Fortinet v5.4.1 10.Fortigate units 60c 與 100D		
影響等級	中		

建議措施	各機關可自行或聯絡設備維護廠商，利用 ICMP 工具，例如 hping3 工具，執行「hping3 -1 -C 3 -K 3 -i u20 」或「hping3 -1 -C 3 -K 3 --flood 」指令進行測試，其中為受測之網路設備。若在測試過程中，造成內部使用者無法連線到外部網路，即代表網路設備受此漏洞影響。請參考以下建議： 1.建議機關評估於防火牆或閘道器設備對外界面網卡(WAN 端)設定阻擋所有 ICMP Type 3 封包，若此影響 IPsec 或 PPTP 連線時，僅再額外開放 ICMP Type 3 code 4 (fragmentation needed)之封包。 2.若設備廠牌為 Palo Alto，則請參考 Palo Alto 官方網頁(http://researchcenter.paloaltonetworks.com/2016/11/note-customers-regarding-blacknurse-report/)之建議措施。 3.其餘設備廠牌目前尚未發布建議措施，所以仍請各機關密切注意各廠牌官方網頁之更新資訊。
參考資料	1.http://researchcenter.paloaltonetworks.com/2016/11/note-customers-regarding-blacknurse-report/ 2.http://www.ithome.com.tw/news/109565 3.http://soc.tdc.dk/blacknurse/blacknurse.pdf 4.https://tools.cisco.com/security/center/publicationListing.x 5.https://www.zyxel.com/us/en/products_services/smb-security_appliances_and_services.shtml 6.https://support.sonicwall.com/ 7.https://blog.fortinet.com/2016/11/14/black-nurse-ddos-attack-power-of-granular-packet-inspection-of-fortiddos-with-unpredictable-ddos-attacks 8.http://www.hping.org/download.html 9.http://www.zyxel.com/tw/zh/support/announcement_blacknurse_attack.shtml

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