教育機構 ANA 通報平台 漏洞/資安訊息警訊

發布編號	ICST-ANA-2014-0020	發布時間	Fri Sep 26 17:59:38 CST 2014
事件類型	漏洞預警	發現時間	Fri Sep 26 00:00:00 CST 2014
警訊名稱	GNU Bash 存在高風險 CVE-2014-6271 與 CVE-2014-7169 (ShellShock)弱點		
內容說明	近期美國國家標準技術研究所(NIST)的國家弱點資料庫(NVD)發布弱點編號 CVE-2014-6271 與 CVE-2014-7169 (ShellShock)，弱點可利用 GNU Bash 的環境變數執行未經授權的任意指令。攻擊者可透過弱點主機上之網路服務，如 web server，發送 HTTP request 和 CGI script，將惡意指令傳送至 Bash，進而使系統自動執行攻擊者所設計的惡意指令。 為確保平台安全性，請各機關確認所屬系統 GNU Bash 版本並儘速修補漏洞，以防止遭受相關攻擊。		
影響平台	作業系統(如：Linux、Unix、Mac OS、Unix-like(包含 Router、Firewall、IPS、IDS、Android 、iOS)等)所使用 GNU Bash 之版本如下： gnu:bash:1.14.0、gnu:bash:1.14.1、gnu:bash:1.14.2、gnu:bash:1.14.3、gnu:bash:1.14.4、gnu:bash:1.14.5、gnu:bash:1.14.6、gnu:bash:1.14.7、gnu:bash:2.0、gnu:bash:2.01、gnu:bash:2.01.1、gnu:bash:2.02、gnu:bash:2.02.1、gnu:bash:2.03、gnu:bash:2.04、gnu:bash:2.05、gnu:bash:2.05:a、gnu:bash:2.05:b、gnu:bash:3.0、gnu:bash:3.0.16、gnu:bash:3.1、gnu:bash:3.2、gnu:bash:3.2.48、gnu:bash:4.0、gnu:bash:4.0:rc1、gnu:bash:4.1、gnu:bash:4.2、gnu:bash:4.3		
影響等級	高		
建議措施	1.建議參考以下方式確認系統 GNU Bash 版本與安全性： [方式 1]確認 GNU Bash 版本 利用"bash --version"檢視 GNU Bash 版本是否為上述影響範圍內。 [方式 2]透過檢測指令確認系統是否存有弱點 CVE-2014-6271 弱點檢測指令： 開啟 shell 執行下列指令(請注意空白需正確輸入) env x='() { :;}; echo vulnerable' bash -c "echo this is a test"		

	若出現以下字串代表該主機存在該漏洞 vulnerable this is a test CVE-2014-7169 弱點檢測指令：目前尚無有效檢測指令 2.如以上述方式檢測確認系統存有 ShellShock 弱點，請盡速至系統官方網站更新 Bash 版本。 3.處理機敏公務之設備，應考量實體隔離原則。 4.若後續有任何弱點更新訊息，將另發更新警訊。
參考資料	1.http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271 2.http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271 3.http://thehackernews.com/2014/09/bash-shell-vulnerability-shellshock.html 4.http://www.securityfocus.com/bid/70103 5.https://discussions.apple.com/thread/6558974 6.http://www.ubuntu.com/usn/usn-2362-1/ 7.http://lists.centos.org/pipermail/centos/2014-September/146099.html 8.https://lists.debian.org/debian-security-announce/2014/msg00220.html