一、弱點知識庫

＊ PHP.Windows.Shell.Escape.Functions.Command.Execution

說明	PHP for Win32 v4.3.6 及之前的版本含有允許遠端攻擊者執行命令的弱點，PHP 提供 escapeshellarg()函數來執行 shell 命令，但因 PHP Windows shell 的 escapeshellarg 函數沒有充分過濾'%|>'字元，遠端攻擊者可以發送特製的 HTTP 請求傳送包含 shell 字元到 Web Server 上來執行任意命令，藉以獲取存取該主機的權限。
影響	遠端攻擊者可取得獲取存取該主機的權限
影響系統	Microsoft Windows 版本的 PHP 4.3.5 和 PHP 4.3.3
建議解決方法	1.檢查防火牆紀錄：查看記錄是否有外界對貴單位內部 IP 之異常連線。 2.如發現為非授權的連線，建議將該 IP 於防火牆阻擋。 3.建議將目前所使用的版本升級到最新。 http://www.php.net/downloads.php
參考資料	**FortiGuard** https://www.fortiguard.com/encyclopedia/vulnerability/#id=10811 **SecurityFocus** http://www.securityfocus.com/bid/10471。 **CVE - Common Vulnerabilities and Exposures** http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-0542

＊DLink.IP.Cameras.rtpd.cgi.OS.Command.Injection

說明	D-Link 的網路攝影機系統中的/var/www/cgi-bin/rtpd.cgi 存有遠端命令執行的漏洞，遠端攻擊者可以透過發送蓄意製作的 http request 至 D-Link 的網路攝影機系統的 web 界面。如成功利用此漏洞，遠端攻擊者可以在受影響的系統上以系統權限執行任意程式碼或導致系統發生錯誤。
影響	遠端攻擊者可取得系統權限執行任意程式碼。
影響系統	DCS-3411/3430 - firmware v1.02,DCS-5605/5635 - v1.01,DCS-1100L/1130L - v1.04,DCS-1100/1130 - v1.03,DCS-1100/1130 - v1.04_US,DCS-2102/2121 - v1.05_RU,DCS-3410 - v1.02,DCS-5230 - v1.02 DCS-5230L - v1.02,DCS-6410 - v1.00,DCS-7410 - v1.00,DCS-7510 - v1.00,WCS-1100 - v1.02
解決方法建議	1.檢查防火牆紀錄：查看記錄是否有外界對貴單位內部 IP 之異常連線。 2.如發現為非授權的連線，建議將該 IP 於防火牆阻擋。 3.更新至最新韌體版本
參考資料	**FortiGuard** http://www.fortiguard.com/encyclopedia/vulnerability/#id=35338 **CVE** http://cve.mitre.org/cgi-bin/cvename.cgi?name=2013-1599 **Exploits Database by Offensive Security** http://www.exploit-db.com/exploits/25138/ **SecurityFocus** http://www.securityfocus.com/bid/59564/

二、惡意程式分析報告

(一) 惡意程式基本資料

1、單一識別碼(Hash 值)

- MD5：7d2682f21bdff7846cd6be9f5737d2bf
- SHA-1：18e747a4c9a409bf349a4aaefd3e255ecf28f039

2、惡意程式檔案大小：308,363 bytes

3、各防毒軟體定義名稱：

- AntiVir：TR/Spy.308363
- BitDefender：Gen:Trojan.Heur.suZ@yP!QOyibf
- Fortinet：W32/Generik.NOKHTPR!tr

(二) 惡意程式行為分析

1、此惡意程式感染主機後會新增惡意程式：%TEMP%\svhost.exe

2、此惡意程式會使用反轉字元與圖示更換的方式，欺騙使用者，開啟偽裝為文件檔的螢幕保護程式：

實際上是一個使用反轉字元技術進行偽裝的螢幕保護程式

3、修改系統啟動程序

此惡意程式會修改機碼，確保每次受害主機重開機後都會執行這個程式：

- <HKLM>\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- <HKCU>\Software\Microsoft\Windows\CurrentVersion\Run

4、修改防火牆規則並嘗試對外連線：受害主機感染惡意程式後會修改本機防火牆規則，允許%TEMP%\svhost.exe 可以對外連線。

(三) 提升本機安全性防護

1、安裝防毒軟體並定期更新病毒碼

建議電腦使用者必須要安裝防毒軟體並定期病毒碼，避免網路威脅發生。

2、開啟本機防火牆並定期安裝系統更新

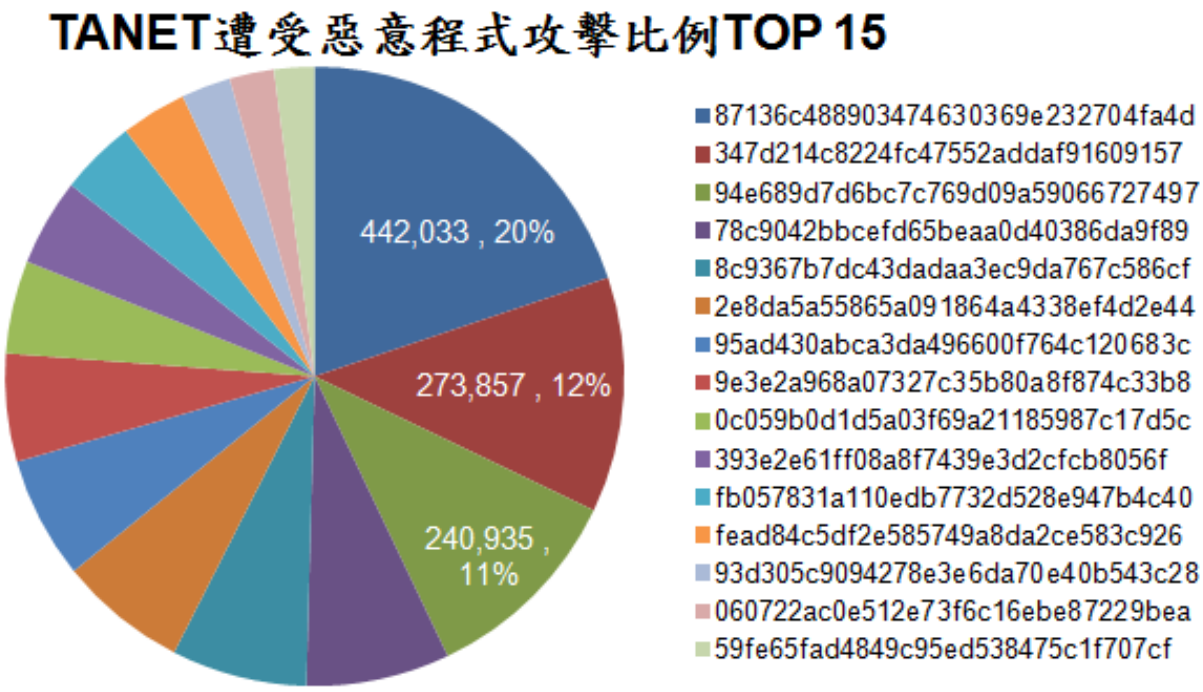
開啟微軟系統內建之系統更新功能，定期針對系統重大更新以及安全性更新檔進行安裝，避免系統暴露在攻擊的威脅之下。

3、惡意程式移除工具

若使用者的電腦系統不慎遭到此惡意程式感染而無法正常運作，請下載各大防毒軟體廠商所釋出之惡意程式移除工具，以進行病毒清除程序。以下網址可供參考

- Microsoft Safety Scanner,官方網站：
  http://www.microsoft.com/security/scanner/zh-tw/default.aspx
- TrendMicro System Cleaner,官方網站：
  http://downloadcenter.trendmicro.com/index.php?regs=TW
- Norton Rescue Tool,官方網站：
  http://tw.norton.com/free-tools-trial/promo

【惡意程式攻擊】



惡意程式名稱	防毒軟體偵測名稱
87136c488903474630369e232704fa4d	Kaspersky:Net-Worm.Win32.Kido.ih McAfee:W32/Conficker.worm TrendMicro:WORM_DOWNAD.AD AVG:Downloader.Generic11.ATTH Symantec:W32.Downadup.B
347d214c8224fc47552addaf91609157	Kaspersky: Net-Worm.Win32.Kido.ih McAfee: W32/Conficker.worm.gen.a TrendMicro:WORM_DOWNAD.AD AVG:Worm/Downadup Symantec: W32.Downadup
94e689d7d6bc7c769d09a5906672749 7	Kaspersky:Net-Worm.Win32.Kido.ih McAfee:W32/Conficker.worm TrendMicro:WORM_DOWNAD.AD AVG:Worm/Downadup Symantec:W32.Downadup

【最易被攻擊的帳號】

TOP	帳　號	次　數
1	root	689,851
2	admin	9,553
3	oracle	2,365
4	test	1,156
5	nagios	1,078
6	bin	964
7	user	848
8	postgres	819
9	mysql	544
10	ftpuser	525

【最易被猜測的密碼】

TOP	密　碼	次　數
1	root	7,136
2	123456	4,653
3	admin	4,317
4	password	2,940
5	test	2,358
6	test123	2,149
7	qwerty	2,026
8	admin123	2,007
9	passwd	1,847
10	changeme	1,524

【最危險的帳號密碼組合】

TOP	帳　號	密　碼	次　數
1	root	admin	3,252
2	root	123456	1,422
3	root	123456789	1,053
4	root	111111	974
5	root	1234	927
6	root	123	924
7	root	123qwe	917
8	root	1234567	844
9	root	12345	817
10	root	0	812