Open SNMP server 的問題

- NOTICE 2019/11/27 網路協進會報告,自2020/02/11(二)起,比照 open DNS 的處理,若偵測為 open SNMP server 將自動阻斷其IP,請使用者務必修正問題,以免網路遭阻斷。阻斷處理,詳「不當網路資訊」]
- 為幫助本校使用者防治 open SNMP server 的問題, 2019/10/16 本頁面上線,以提供更多相關資料。
- 由於軟體及設備種類繁多,歡迎知悉某特定軟體或設備其修正方法者,能不吝提供資料,嘉惠眾人,
 - 詳:資訊設備[]
 - 若不會用到 SNMP□建議可直接關閉此服務。
 - > 若要用 SNMP□請設定 Access Control List 限制內網存取,或將預設的 community public 改掉,以避免遭濫用。

問題概述

- Open SNMP server 指伺服器(或資訊設備)對外公開且不限使用對象提供 SNMP 服務,可能產生以下 問題:
- 1. 暴露於外界,容易被攻擊或平白損耗系統及網路資源
- 2. 容易被外界利用,成為發動 DDoS 網路攻擊的一員
- 3. 因系統資訊揭露,衍生入侵問題
- 關於利用 SNMP 的反射放大攻擊(reflection and amplification attack)□請參閱此連結 Reflections on reflection (attacks)

偵測系統

□=□□為防治 open SNMP server 問題,協助處理校園內電腦或資訊設備,因設定不慎而可能遭攻擊者利用來 發動網路攻擊,故本組建置 open SNMP server 偵測系統,並將偵測結果提供各單位網管,以便轉知其使 用者參考建議作法來修正設定及自行檢測問題是否解決,藉以減少本校網路內 open SNMP server 的數量。

最近七天內偵測結果

• NOTICE 若已存在本清單的 IP 地址,至少需等待至隔日系統重新偵測,通過後時才會移除,故擬移 出本清單者,請先用下方的「即時檢測服務」,檢查確認該 IP 地址已無問題後,隔日應可自清單中 移除。

更新時間[]Tue Feb 13 09:15:00 2024 Asia/Taipei

序號 單位 ⅠP 位址 偵測時間 備註 總計 0 筆記錄

即時檢測服務

□□□為方便本校使用者自行檢測其電腦或網路設備是否具有 open SNMP server 的問題,特建置此即時的 檢測服務,目前限由本校 IP 位址來進行檢測。(2019/10/02上線試用)

檢測 open SNMP server IP 位址: 1.1.1. . & Anbsp 0000 000

• NOTICE 檢測前請先確認目標 IP 位址的電腦或設備狀態為開機且網路連線正常,以免影響檢測結果。

• 採用 http://opensnmpproject.org/ 的偵測方法,若有類似以下輸出結果,則表具有 open SNMP

檢測說明

server 問題 ○ 不應回覆 SNMP 查詢 Check open snmp for the target IP 140.114.XX.XX Time: Wed Oct 2 09:40:32 2019 check open snmp: 140.114.XX.XX check open snmp server with (140.114.XX.XX,,) Command: /bin/snmpwalk -v 1 -c public 140.114.XX.XX .1.3.6.1.2.1.1 STDOUT: 6 SNMPv2-MIB::sysDescr.0 = STRING: HP ETHERNET MULTI-ENVIRONMENT, ROM R.22.01, JETDIRECT, JD95, EEPROM R.24.06, CIDATE 10/17/2002 SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.11.2.3.9.1 DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (109520430) 12 days, 16:13:24.30 SNMPv2-MIB::sysContact.0 = STRING: SNMPv2-MIB::sysName.0 = STRING: NPI97XXXX SNMPv2-MIB::sysLocation.0 = STRING: SNMPv2-MIB::sysServices.0 = INTEGER: 64 STDERR: -1 Is 140.114.XX.XX an open snmp server? ANSWER: YES for 140.114.XX.XX • 若類似以下輸出結果,表不具有 open SNMP server 問題 1. 無 SNMP 回應, 若電腦已開且網路已通, 則此機無問題。 Check open snmp for the target IP 140.114.63.252 Time: Wed Oct 2 09:45:36 2019 check_open_snmp: 140.114.63.252 check open snmp server with (140.114.63.252,,) Command: /bin/snmpwalk -v 1 -c public 140.114.63.252 .1.3.6.1.2.1.1 STDOUT: -1 STDERR: 0

Is 140.114.63.252 an open snmp server? ANSWER: NO for 140.114.63.252

建議作法

- 若不會用到 SNMP□建議可直接關閉此服務。
- 若要用 SNMP[]至少將預設的 community public 改掉,以避免遭濫用。

防火牆作法

- 以防火牆來限制 SNMP 查詢,預設攔阻 161/udp 的封包,再針對開放服務範圍的 IP 位址來開放服務,這種作法效益最好。
 - NOTCE3用外部間道型防火牆來保護內部所有資訊設備的方法甚為簡便,但考慮到閘道型防火 牆總有需 bypass 或下線的時候,所以平時最好還是將每部資訊設備本身的安全防護做好來。

SNMP 軟體

- 若不會用到 SNMP□建議可直接關閉此服務。
- 若要用 SNMP□至少將預設的 community public 改掉,以避免遭濫用。
 - 。例如: net-snmp 設定檔 snmpd.conf,將以下預設值

rocommunity public

修改 public 為 xxxxxx (自訂不要外流),並限定 140.114.63.0/24 才能連線。

rocommunity xxxxx 140.114.63.0/24

資訊設備

NOTCE有些資訊設備(如:網路印表機、無線網路閘道器□IP分享器、或路由器)本身可能具有 open SNMP server 問題,需適當調整設定或以防火牆來處理,由於資訊設備的類型繁多,若您知悉某裝置該如 何處理,歡迎提供設備廠牌、型號、軟(韌)體版本、及其設定方式的畫面,寄至 mucheng **Cc.nthu.edu.tw**□以利製成以下網頁,嘉惠眾人,格式及文字可參考以下作法,謝謝!

Apple Airport routers

How to disable SNMP on Apple Airport routers

DELL 遠端存取控制器

• N= DELL 伺服器的 iDRAC 9 (Integrated Dell Remote Access Controller 9) 遠端存取控制器:避免

open SNMP resolver 問題之設定方式請參考下圖(2019/10/18)。

 • 進入 Configuration > System Settings > SNMP Traps Configuration > SNMP Settings□將
 Community String 的預設值 public 改掉。

Dashboard 🛛 📱 System 🗸 🛛 🛢 Storage 🗸	Configuration V	🖂 Maintenance 🗸	● iDRAC Settings ~	🔒 Open Group Manager 📼	
Alert Destination 8		None	• Send	Send	
Community String*	public				
SNMP Alert Port Number*	162				
SNMP Trap Format	SNMP v1 .				
	Apply Discard				

Extreme 交換器

- INTERPORT INTERPORT Extreme 交換器:避免 open SNMP resolver 問題之設定方式請參考以下,本資料感謝工科系何 孟軒先生提供(2022/10/21)
 - 參考

https://www.plixer.com/blog/extreme-networks-enabling-and-disabling-snmpv1-snmpv2-a nd-snmpv3/

1. 以下三行新設定一個 SNMPv3 的身分

```
configure SNMPv3 add user <user> authentication md5 <authpassword>
priv des <privpassword>
configure SNMPv3 add group <group> user <user> sec-model usm
configure SNMPv3 add access <group> sec-model usm sec-level priv
read-view defaultAdminView write-view defaultAdminView notify-view
defaultAdminView
```

2. 接著三行取消原本預設的身分跟群組

```
disable SNMP access SNMP-v1v2c
disable SNMPv3 default-user
disable SNMPv3 default-group
```

Press the <tab> or '?' key at any time for completions.</tab>								
Remember to save your configuration changes.								
X430-24t.1 # configure SNMPv3 add user authentication md5								
65 privacy des								
* X430-24t.2 # configure SNMPv3 add group								
* X430-24t.3 # configure SNMPv3 add access sec-model usm sec-level priv								
read-view defaultAdminView write-view defaultAdminView notify-view defaultAdminV								
iew								
* X430-24t.4 # disable SNMP access SNMP-vlv2c								
* X430-24t.5 # disable SNMPv3 default-user								
* X430-24t.6 # disable SNMPv3 default-group								

3. 驗證是否成功

show management

* X430-24t.7 # show management	
CLI idle timeout	Enabled (20 minutes)
CLI max number of login attempts	3
CLI max number of sessions	8
CLI paging	Enabled (this session only)
CLI space-completion	Disabled (this session only)
CLI configuration logging	Disabled
CLI scripting	Disabled (this session only)
CLI scripting error mode	Ignore-Error (this session only)
CLI persistent mode	Persistent (this session only)
CLI prompting	Disabled (this session only)
Telnet access	Enabled (tcp port 23 vr all)
	Access Profile : not set
SSH Access	ssh module not loaded.
Web access	Disabled (tcp port 80)
	Access Profile : not set
Total Read Only Communities	1
Total Read Write Communities	1
RMON	Disabled
SNMP access	v1,v2c Disabled, v3 Enabled,
	v3DefaultGroup Disabled
	ACCESS FIOILIE : NOU SEU
SNMP Traps	Enabled
SNMP v1/v2c TrapReceivers	None

HP 網路印表機

• Imm HP LaserJet M506 網路印表機:避免 open SNMP resolver 問題之設定方式請參考下圖,本資料 感謝醫環系黃竫雯小姐提供(2019/10/25)

С	進	λ	絲	朙路	> 網路設定	> SNM	P□不要	「啟動□SNMP∨	/1/v2 及	z SNMPv3[]
		0		1841	241134					

HP LaserJe	n MSON				111 I
ands salved	10				
	28 Martin Martin Mathematica 2019				
•	鼓翼状態				
	dimense.				
	R.H.				
t.	RAUSE	1997			
10112	10.014070010				
1	1228-848163670		B. CONTRACTOR OF		
in the second	-		The second secon		
6	11111				
	1994	L190	10.84	- 44	0.785
	2000	land 42	100 804	14	141
	and a second			184	
			with the second		

6 1 C A *#1	(141114 memory institute)	4 2 4 1	0 5
🕼 HR Lavet Jet		and a state of the	
APRETAAN 142 PA TO THE			
	THE OWNER AND A REPORT OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTIONO		
82 Totor (2) 97024 4704 87025 8729 802 970 970 970 970 970 970 970 970	MRREE Same		
	NUMBER OF THE TRANSPORT		-

Fuji Xerox 網路印表機

- ▶ Fuji Xerox DocuCentre-VI C3370 網路印表機:避免 open SNMP resolver 問題之設定方式請參考下圖,本資料感謝醫環系黃竫雯小姐提供(2019/10/25)
 - ○進入內容>通訊協定設定>SNMP□不要「啟動」。

← → Q · (D · Fille: 3404343	HA2nial res-		
Centrellane Systemat Services		DesiGente vi CUTII	A MARKET & A DOLLAR
NB 25		11	
	一般		
28년 2011년 - 1 18년 - 승규에 2년 841년			
		ME-WET RECEIPTIONE	
		PEADIN BUS UNKA	
		FUER XIBROX 🌒	
		Traine films Instant Der son the David Science 427 C2017 III EE 1.1 EFrag: Science File. 2011	

		peo-exponing	
Internet Services		Desident d CTR	A 88774 - 32.01
BA 1 25	1 10 1 10 1 10 ME 1 10		
2724	SNMP		
+	£		
- MERE #2500	a and (color).	Case	
******	1021		1
100	Ferminates	sad there - that	
107	G RESERVER	(100 mov -+)	
1008	ERONZEZANX · HREEMoona berindikenyeris		
A278-11	TENENAN		
+ 1.0×12	See		
- POK3 3(019	1222ARR-RGHRM(
108468823		AMMENTS MAKE INS.	
1947 Decemp			
Bagest			
100 Martine			
FTF Automatic			
Magan .			
+ MU22			
+#28			
		and a second	
		LOTINGLOW ®1	
		Contesting instant Research Description (CODE) (#11)	

- N=■ Fuji Xerox DocuPrint CM305 df 網路印表機:避免 open SNMP resolver 問題之設定方式請參考下圖(2019/10/18)。
 - • 進入 Properties > Protocol Settings > SNMP□再 Edit SNMP properties□將所有的
 Community Name 預設值 public 改掉。

CentreWare Internet Services	DocuPrint CM305 df	2
Status Jobs	Address Book Properties Printer Support	
	C Protocol Settings SNMP Configuration C Enable SNMP v1/v2c Protocols C Enable SNMP v3 Protocols C Enable sitter SNMP v1/v2c or SNMP v3	NMP v1/v2c Properties
SMB Tahet SMMP Ubdate Address Book Ubdate Address Book DAP Server DAP User Mapping - B ETP Chent SMB Crisert	Enable HTTP'S to edit the SNMP v3 protocol. Apply Und FUJI XEFOX	•
CentreWare Internet Services	DocuPrint CM305 df	2 Entr
Control Settings Cont		-
Bergenergenergenergenergenergenergenerge	Community Name (Read only) Re-enter Community Name (Read Only) Community Name (Read/Write) Re-enter Community Name (Read/Write) TRAP Community Name Re-enter Community Name Re-enter Community Name (Trap Notification)	
Update Address Book UDAP Server UDAP User Mapping FTP Chest Got Skill Chest	Configuration1	•

Ricoh 網路印表機

● New Ricoh SP C252SF 網路印表機:避免 open SNMP resolver 問題之設定方式請參考下圖,本資料

感謝긔 ∘	【科系何孟軒5 進入 網路設定	も生提供(202 ミ > SNMP >	0/02/10 設定	0) SNMP⊡	無效」	0					
	RICOH	SP C252SF			Web image monitor						
	首頁	網路設定									
	系統設定										
	單鍵撥號目的地		網	路狀態	IPv6設	置	網路應用程式	DNS	自動電子郵件通知	SNMP	
	掃描目的地										
	傳真快速撥號目	的地	Chill	40							
	特殊傳送者		SNI	мР							
	限制可用功能		S	SNMP		: 0	有效 🖲 無效	t			
	網路設定		Trap								
	IPsec設定		目標Tran			: 0	有效 💿 無效	ł			
	列印清單/報告			NMD	田十 ## 1	_					
	管理員工具			DNMP EX	王主领工	-					
			• 2	NMPER	<u>至土機</u> 2	:)					
			社都	¥							
				Get社群		:publ	ic				
			= 1	「rap社群		:					
			系統	ŧ							
			= f	立置		:					
			= 1	聯絡		:					
			請輸	入管理員	密碼。	P					
				確定			取消				

Sharp 網路印表機

- ■ Sharp MX-M314N 網路印表機:避免 open SNMP resolver 問題之設定方式請參考下圖,本資料 感謝體育室鄧智予先生提供(2020/02/26)
 - ◎ 進入 埠號控制 > 將「伺服器埠號」的 SNMPD□設定為「禁止」。

9/10

- 7 G A 798	HE114.184 (Synourby portners)		Ý 🗧
MX-M314N	埠號控制		
	BH25(3) #F25(R)		
RELY	州寨营华性		
1738	HETP	DO · HORSER III (CANNO)	
1212.0030	HETPS	De . augusta (1) (04660)	
THE O	FTP 594	20 · emplois 21 (046606)	
10970	Raw P(E):	20 · #0958 910 (04053)	
a ristal	LPD:	BR * 00958 515 (0-0500)	
	PP.	2020 * 00000000 8371 (0-69500)	
AND/O	PP-101.	第22 * 編編単数第 (421 (0-66436)	
254.00	3425A/1mits	Ball * Jergerstreff (2000 (0-66536)	
意用取 从設置	SWIPD	1842 *	
E-mail @ 9.2.2.2.2	TELNET:	and the second se	
27802	METOVINE	mit."	
A STATE	JCP.	第12 *	
OCCUPATION NOTICE OF	RAND .	Hit ·	
- FRAME	980	BR ·	
1 1010/2214	TOB.	HR.	
- Martiner	用户标准数		
55.RE	HEIR	PD 1	
Field	HTTPS	88.	
0.071000	FTP	80.1	
	FTRk	28 *	
	SHIP.	inter •	
	SHTP-55L	ing •	
	POP3	200 *	
	P073-55L	20.1	
	SNIRP TRAP	H	
	提示工作描述:		
	LENP	2.0.	
	LLWP-SOL: Kalik-Alin-K	21 ·	
	SWITE	He .	
	aChile	(The later of the	

KYOCERA

• KYOCERA□避免 open SNMP resolver 問題之設定方式請參考下圖,本資料感謝工科系何孟軒先生提供 (2021/06/25)

○ 進入 網路	{>網路設定:	> 協定 > 其他協定	,不要	「啟動[]SNMPv1/v2c 乃	ἑ SNMPv3[
---------	---------	-------------	-----	-------------------	-----------

Kyocera Col	m	nand Center	Econs .	型號:ECOSYS M5520.cdn E機名稱:KM9CF623 位置:	
1 主重直		《 網路設定 : 協定	2	:吹更新時間: 021/06/25 12:35:56	C
Admin					
登出		協定設定			
		列印協定			
	_	"NetBEUI :	(1) 開設	○開閉	_
設備資訊 / 還端操作	>	*網域 / 工作群组:	KM-NetPrinters	<u> </u>	
作業狀態	>	*註解:			
	_	"LPD :	(1) 開設	○開閉	_
又件貞科重		*FTP 伺服器(接收):	● 開啟	○開閉	_
包地址簿	>	"IPP :		○開閉	
P # # # # #	>	"連接埠編號:	631 (1 - 32	767)	
	-	*IPP over SSL :	● 開欽	〇開閉	
	>		<u>注意</u> : 要使用這些設定。	請欽用 SSL ・ <u>網路安全</u>	
「「「「「「「」」「「」」「」」「」」「」」「」」「」」「」」「」」「」」「」	~	*連接埠編號:	443 (1 - 32	767)	
- 62		*IPP over SSL憑證:	設備憑證 1		
TCP/IP			設定		
└→ 協定		IPP 驗證:	○ 開政		

*SNIMDv1/v2c ·	
SINNEY IVZC .	○ 開取 ● 開闭
	注意:
	有關詳細設定,請按一下這裏。 <u>SNMP 設</u>)
*SNMPv3 ·	

參考資料

• Open SNMP Project

From: https://net.nthu.edu.tw/netsys/ - 網路系統組

Permanent link: https://net.nthu.edu.tw/netsys/snmp:open_snmp

Last update: 2022/10/21 10:36

