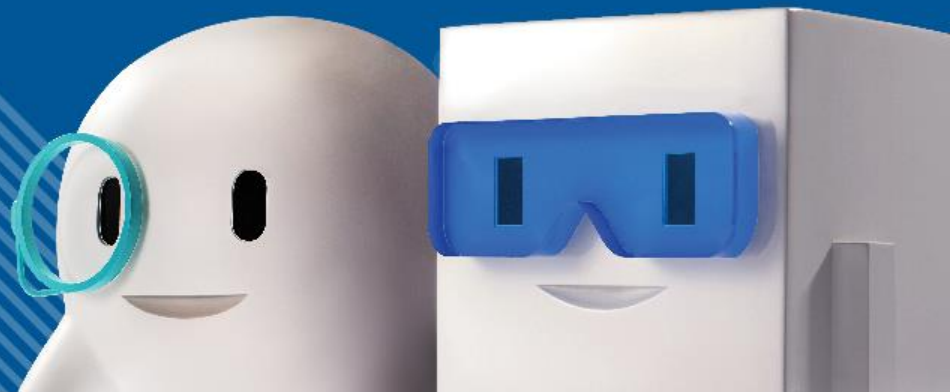




HKPC[®]

智能家居的保安心法

Marco Ho
Security Analyst
HKCERT



Hong Kong Computer Emergency Response Team Coordination Centre



- ▶ 本中心成立於 2001 年
- ▶ 由 香港特別行政區 政府支助
- ▶ 由 香港生產力促進局 負責營運
- ▶ 角色
 - ▶ 服務本地的互聯網用戶、非政府組織、學校、中小企和企業
 - ▶ 保安事故的國際聯絡點

我們的服務

- ▶ 警報監測及預警
- ▶ 事故處理及支援
- ▶ 發放保安指南及資訊
- ▶ 提高資訊保安意識

你可向我們尋求協助

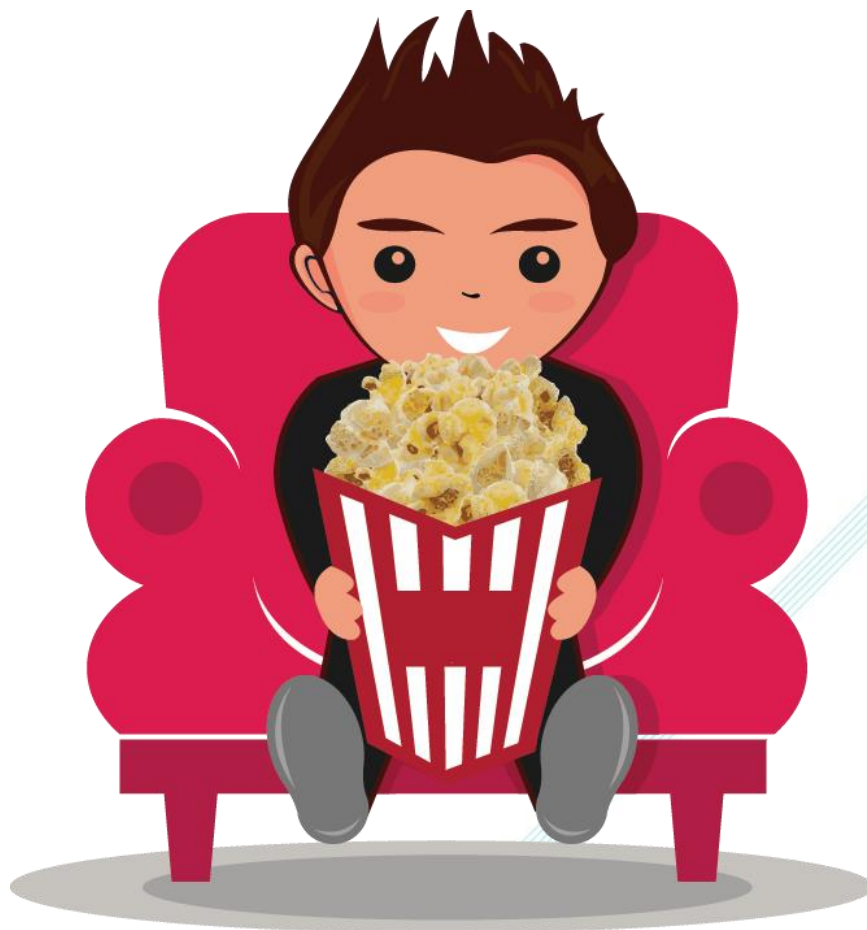
- ▶ 網址：<https://www.hkcert.org>
- ▶ 電話熱線：**[852] 8105 6060**
- ▶ 電郵：hkcert@hkcert.org

何為智能？



- ▶ 自動化
- ▶ 監測及控制
- ▶ 即時
- ▶ 提供建議
- ▶ 提早為你安排

何為智能？



何為智能？



- ▶ 自動化
- ▶ 監測及控制
- ▶ 即時
- ▶ 提供建議
- ▶ 提早為你安排

常見的智能設備

- ▶ 網路攝影機 (**IP CAM**)
- ▶ 寬頻路由器 (**Broadband Router**)
- ▶ 網路儲存伺服器 (**NAS**)



其他的智能設備

- ▶ 智能燈光系統 (燈泡／開關制)
- ▶ 智能溫度控制系統 (溫度感應器／紅外線收發器)
- ▶ 智能電源插座



易被忽略的智能設備

- ▶ 智能門鎖
- ▶ 吸塵機器人
- ▶ 門禁／窗禁系統
- ▶ 智能玩具



一般連線方式及控制方法

► 網路連線

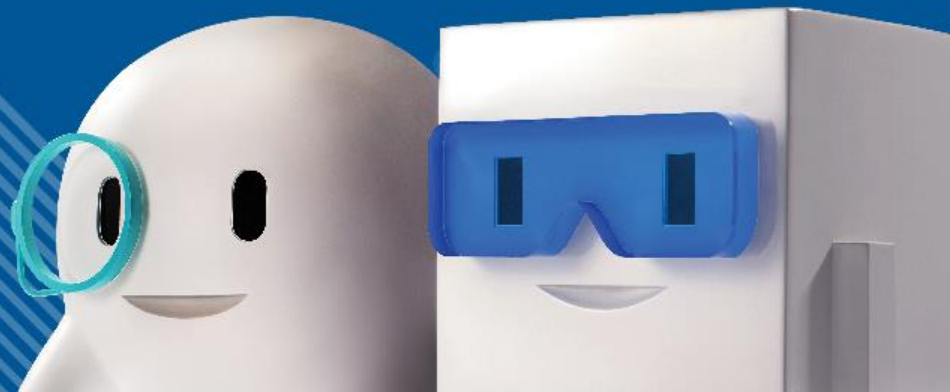
- 有線
- 無線

► 控制的方式

- 使用手機應用程式
- 使用預設的控制台
- 使用雲端系統



智能家居的保安問題



Get Latest Articles to Your Inbox [Subscribe Now!](#)

[Home](#) [Hacking](#) [Tech](#) [Deals](#) [Q](#)

 **The Hacker News**™
Security in a serious way

Friday's Massive DDoS Attack Came from Just 100,000 Hacked IoT Devices

📅 Wednesday, October 26, 2016 👤 Swati Khandelwal

[G+](#) 45 [Like](#) 2.5K [Share](#) 1164 [Tweet](#) 309 [in Share](#) 136 [Share](#) 1678

Analysis Of Friday Attack

Future DDoS Attacks Could Reach 10 Tbps

Guess how many devices participated in last Friday's massive DDoS attack against DNS provider Dvn that caused vast internet outage?
thehackernews.com/2016/10/ddos-attack-mirai-iot.html

- ▶ **Mirai**（未來）惡意程式
- ▶ 感染了過十萬隻網路攝影機
- ▶ 在 2016年 9月至 10月之間發出了三次阻斷服務攻擊
- ▶ 利用預設的管理員帳號入侵

CLOUD

Synology NAS devices targeted by ransomware

Users of Synology NAS systems are being targeted by ransomware that is demanding payment in exchange for the encryption keys to their files. Here's how they can protect their data.

By James Sanders | August 4, 2014, 6:42 PM PST

Recommended Content:

Downloads: Manage Logs, Fix Problems, Solve Issues, Save Time with SolarWinds Log & Event Manager

When your network is being attacked response time is critical and you need answers fast. SolarWinds® Log & Event Manager makes finding answers easy by providing an easy-to-use virtual appliance which can be downloaded and installed in less than an...

[Download Now](#)

2

f 61

in 11

t

≡



WHITE PAPERS, WEBCASTS, AND DOWNLOADS

White Papers // From NetApp

Will Your Data Benefit from a Cloud Consumption Model?



This eBook examines some of the reasons for moving to a consumption model for IT and reviews the three types of NetApp storage offerings that can be purchased using this type of model: cloud data services, cloud connected storage, and on-demand storage services.

[DOWNLOAD NOW](#)

White Papers // From NetApp

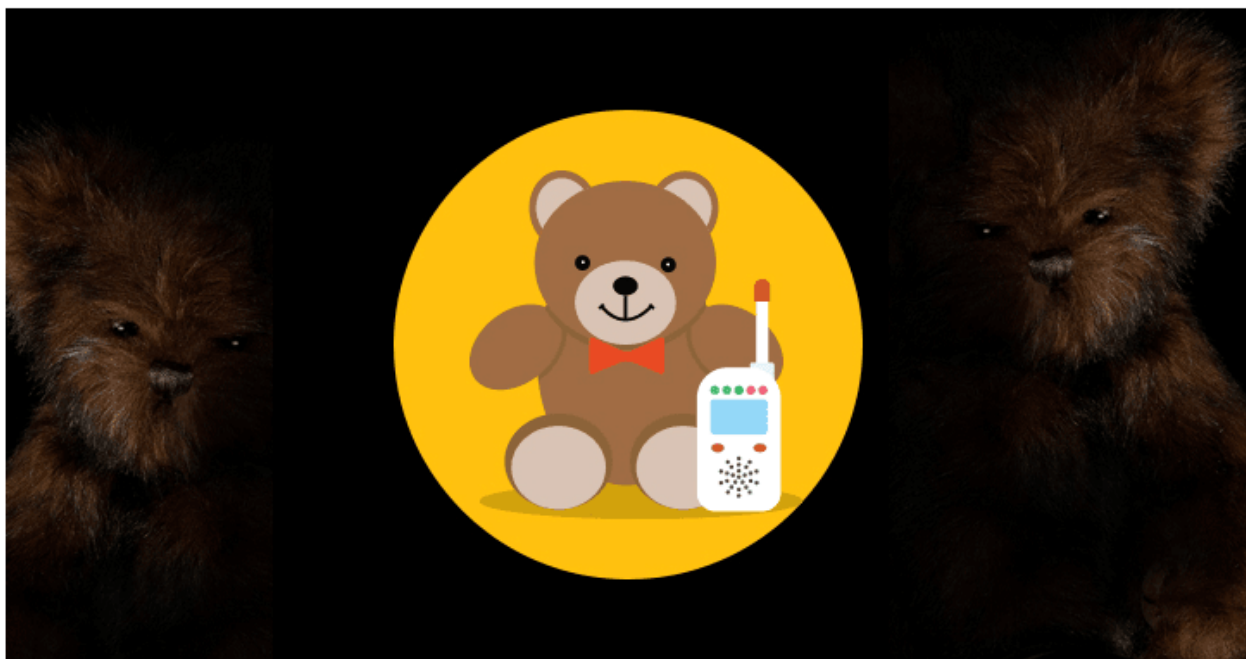
Hybrid Cloud Is The Foundation For Storage Agility And Economics (Forrester report)

[DOWNLOAD NOW](#)

Internet-Connected Teddy Bear Leaks Millions Of Voice Messages and Password

Monday, February 27, 2017 Swati Khandelwal

[Tweet](#)
[G+ Share](#)
[Share](#)
45
[in Share](#)
701
[Share](#)
2.9k
[Share](#)



Every parent should think twice before handing out Internet-connected toys or smart toys to their children, as these creepy toys pose a different sort of danger: **privacy and data security risks** for kids who play with them.

普遍智能設備的問題

- ▶ 系統存在漏洞
- ▶ 保安設施不足
- ▶ 預設密碼太簡單或不能更改
- ▶ 沒有提供韌體更新
- ▶ 預設開啟了遠端控制服務 (**Telnet/SSH**)



購買上的留意事項



- ▶ 品牌的信用度
- ▶ 過去的事故及處理方法
- ▶ 韌體更新的密度

搜尋保安事故

D-Link
Building Networks for People



首次設置

讓我們告訴您怎麼做！



產品註冊



聯繫技術支援

通過電話或電子郵件獲取幫助

DIR-850L

Wireless AC1200 雙頻Gigabit



下載

常見問題

教學影片

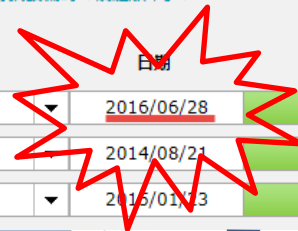
規格

為了獲得正確的下載，請為您的設備選擇正確的硬體版本。

B1

[如何尋找設備的「硬體版本」？](#)

類型	日期			
DIR-850L韌體 (2.07)	2016/06/28	下載	檔案說明	發行說明
SharePort Plus Utility 使用手冊(英文) (4.01)	2014/08/21	下載	檔案說明	
SharePort Plus Utility (Mac作業系統) (4.60)	2015/01/13	下載	檔案說明	發行說明



並沒有立即堵塞漏洞

POPULAR D-LINK ROUTER RIDDLED WITH VULNERABILITIES

by Tom Spring

September 11, 2017, 2:09 pm

A wireless router made by D-Link has nearly one dozen critical vulnerabilities, according to a report released by independent researcher Pierre Kim.

檢查韌體更新

EA7500 Downloads



支援產品

RT-AC66U

[選擇其他產品 >](#)

驅動程式及工具程式

常見問題

手冊及文件

IMPORTANT: Before downloading, it is highly re

Your router must have an internet connection pri

Select your hardware version:

▼ Version 2.0

FIRMWARE

Ver. 2.0.3.181171

Latest Date: 06/14/2017

[Download](#) 31.6 MB

[Release Notes](#)

IMPORTANT: The EA7500 v2 firmware is not compatible with the EA

驅動程式及工具程式

BIOS及韌體

持續提供更新

需要協助?

[聯絡我們_客服中心](#)

版本 3.0.0.4.380.7743

2017/06/26 更新 29.89 MBytes

ASUS RT-AC66U 韌體版本 3.0.0.4.380.7743

安全性修正

- 修正CVE-2017-8828 (XSS漏洞, 感謝 Yair Amit's <https://www.linkedin.com/in/yairamit/> 的貢獻)
- 修正CVE-2017-5892 (JSONP 資訊洩漏)
- 修正CVE-2017-7494 (Samba 遠端執行漏洞)
- 增強SSH, Telnet 連接對暴力攻擊的防護

其餘購買上的留意事項



- ▶ 閱讀使用者手冊
- ▶ 留意加密連線（管理者介面）
- ▶ 留意保安設定
- ▶ 是否容易進行韌體更新
- ▶ 是否容易安裝／設定



支援產品
RT-AC68U

[選擇其他產品 >](#)

快速存取您的產品清單

[註冊您的產品](#)

預先下載使用手冊 並瀏覽當中的安全設定

驅動程式及工具程式

手冊及文件

保固條款

手冊及文件

無線網路安全設定

為了保護您的無線網路以免非授權使用者侵入，您需要進行無線網路安全設定。

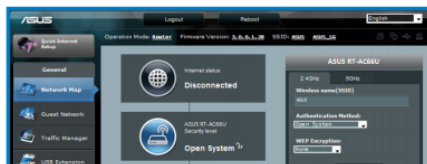
請依照以下步驟進行無線網路安全設定：

1. 在您的網頁瀏覽器中輸入 **192.168.1.1**。
2. 在登入頁面中，輸入預設使用者名稱（admin）與密碼（admin），然後點選 **確定**。無線路由器的網頁圖形介面開啟。
3. 在 **網路地圖** 畫面中，選擇 **系統狀態** 圖示以顯示無線安全設定，如 SSID、安全級別與加密設定。



注意：您可以為 2.4GHz 與 5GHz 頻進行不同的無線網路安全設定。

2.4GHz 安全設定



版本 20170613
2017/06/14 更新 183.26 KBytes

[下載](#)

RT-AC68U EU Declaration of Conformity (Spanish)

版本 20170613
2017/06/14 更新 242.91 KBytes

[下載](#)

RT-AC68U EU Declaration of Conformity (French)

版本 20170613
2017/06/14 更新 183.37 KBytes

[下載](#)

RT-AC68U EU Declaration of Conformity (Portuguese)

智能設備上的留意

- ▶ 安裝在內聯網 (**LAN**)
- ▶ 建立分離網絡
- ▶ 關閉通用隨插即用 (**UPnP**) 功能
- ▶ 保持韌體更新

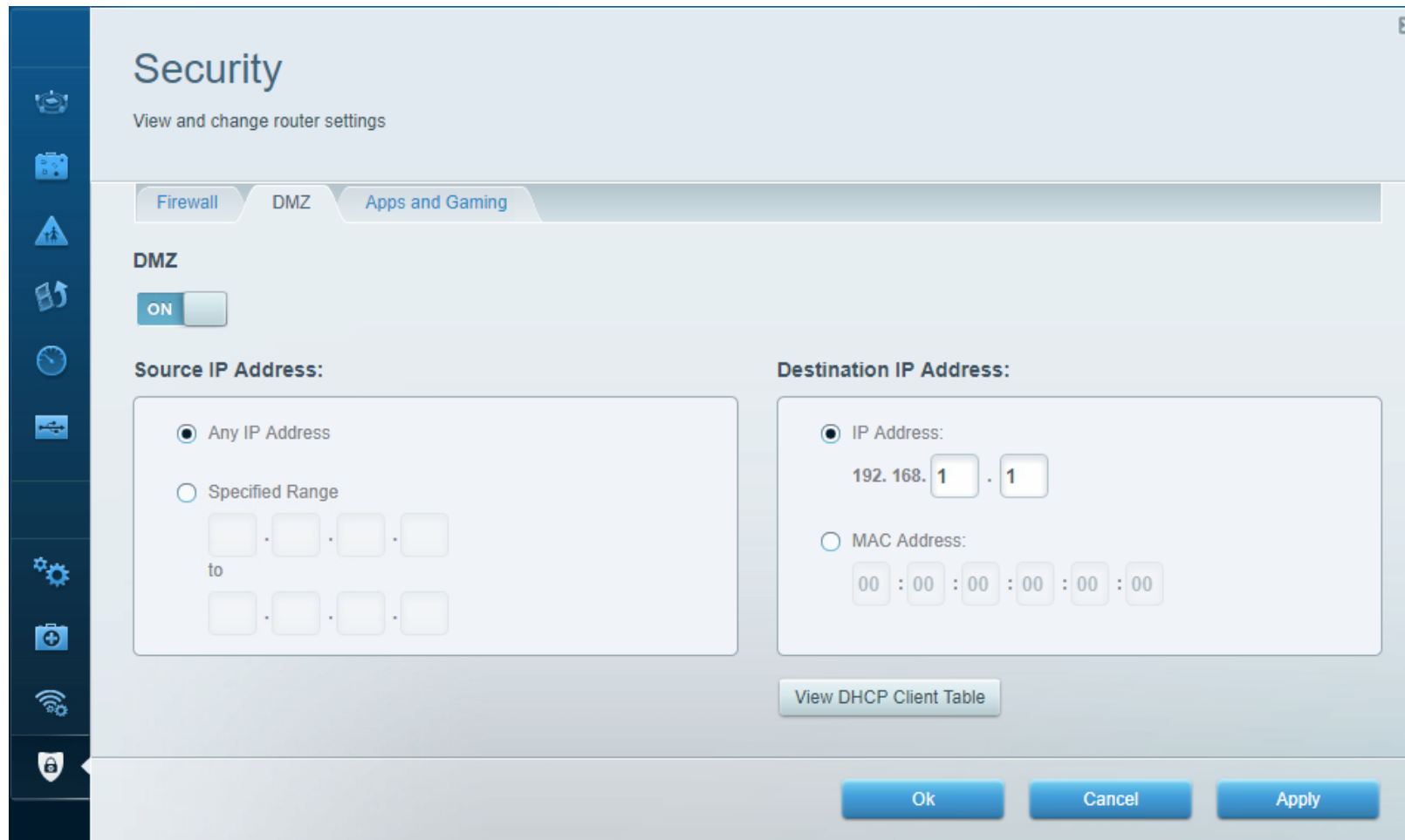
智能設備上的留意

- ▶ 使用強健的密碼
- ▶ 管理介面不應向互聯網開放
- ▶ 是否必需連接雲端
- ▶ 不常用的設備(如 **SmartTV**)，請拔除網絡連線



在家庭的環境，寬頻路由器是你最前端的防護

留意 DMZ 的設定 (是否必需)



The screenshot shows the 'Security' configuration page of a router, specifically the 'DMZ' tab. The page title is 'Security' with the subtitle 'View and change router settings'. The 'DMZ' tab is selected, and the 'DMZ' toggle switch is turned 'ON'. Under 'Source IP Address', the 'Any IP Address' radio button is selected. Under 'Destination IP Address', the 'IP Address' radio button is selected, and the IP address '192.168.1.1' is entered in the provided fields. The 'MAC Address' radio button is unselected. A 'View DHCP Client Table' button is located below the IP address fields. At the bottom right, there are 'Ok', 'Cancel', and 'Apply' buttons.

Security
View and change router settings

Firewall DMZ Apps and Gaming

DMZ

ON

Source IP Address:

☒ Any IP Address

☐ Specified Range

to

Destination IP Address:

☒ IP Address:

192.168.1.1

☐ MAC Address:

00 : 00 : 00 : 00 : 00 : 00

View DHCP Client Table

Ok Cancel Apply

使用 Single Port forwarding 功能



Security

View and change router settings

Firewall
DMZ
Apps and Gaming

DDNS
Single Port Forwarding
Port Range Forwarding
Port Range Triggering

Application name	External Port	Internal Port	Protocol	Device IP#	Enabled	
EasyN Cam	9000	81	TCP	192.168.0.29	True	Edit/ Delete
DS_BT	8080	9004	TCP	192.168.0.253	True	Edit/ Delete
DS_FTP	8081	9005	TCP	192.168.0.253	True	Edit/ Delete
BT_Port1	16881	16881	TCP	192.168.0.253	True	Edit/ Delete
BT_Port2	6881	6881	UDP	192.168.0.253	True	Edit/ Delete
BT_Port3	1701	1701	UDP	192.168.0.253	True	Edit/ Delete
BT_Port4	4500	4500	UDP	192.168.0.253	True	Edit/ Delete
BT_Port5	500	500	UDP	192.168.0.253	True	Edit/ Delete

Add a new Single Port Forwarding

Ok
Cancel
Apply

新思維的路由器設備

F-SECURE SENSE

The missing piece of your connected home

[Buy now](#)

[Watch video](#)

Easily secure every connected thing in your home using one device, now and in the future. F-Secure SENSE is the combination of a security router, an advanced security app and industry-leading cloud protection.



Introducing Norton Core™

Locks down connected devices in your home against cyber threats.

- A stylish and powerful router for your connected home
- Integrated with Norton Security
- Easy to manage

PLUS FREE SHIPPING

Buy from:

See below for details



Bitdefender

[COMPARE](#) [SETUP](#) [SUPPORT](#)

Smart security for all your connected devices.

[FIND OUT MORE](#)



“Bitdefender BOX is every computer, p



網站地圖 | 確認本網頁的身份  中文 | English AAA  搜尋...

香港電腦保安事故協調中心

關於我們 | 警報及消息 | 服務 | 刊物 | 資源 | 手機 Apps / 流動版 | RSS

警報及消息 » 保安博錄 »

警報及消息

保安公告

保安博錄

相關新聞

保安博錄

智能設備購買及安裝小貼士

發布日期: 18 / 09 / 2017

最後更新: 18 / 09 / 2017

   Share  Tweet

[60 觀看次數]

近年互聯網及物聯網 (Internet of Things, IoT) 的設備快速增長，有報告預計在 2020 年相關的設備會增長到約全球 210 億件，相信相關設備好快會超越個人電腦的數量。而在對上的一年，黑客留意到這些設備有很多都存在著保安漏洞或問題，就在 2016 年的 9 月及 10 月入侵了部份有保安問題的設備並進行大規模的阻斷服務攻擊，而所利用惡意程式名叫 "Mian" #1，這次攻擊告訴了我們互聯網及物聯網設備已經成為新一代的網絡攻擊利器。

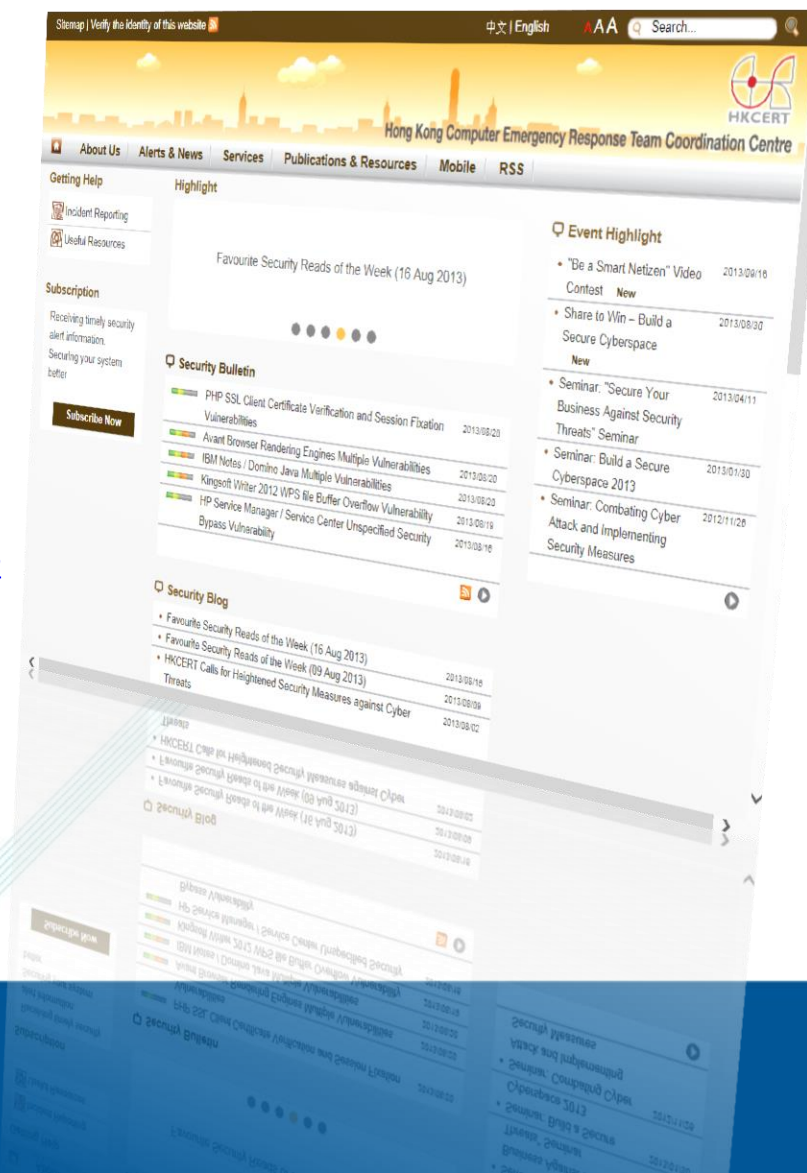
經過此事故後，多個保安團隊也紛紛研究全球有多少這些有保安問題的設備，所得出的結果也是遠超想像。本中心也在 2015 至 2016 年之間進行了一系列有關互聯網及物聯網設備的專題研究 #2，也發現為數不少的設備直接向互聯網開放，而部份設備也存在保安問題。

智能設備購買及安裝小貼士

https://www.hkcert.org/my_url/blog/17091801

HKCERT 的保安指南及手冊

- ▶ 保安指南
 - <https://www.hkcert.org/security-guideline>
- ▶ 保安工具
 - <https://www.hkcert.org/security-tools>
- ▶ 手機保安工具
 - <https://www.hkcert.org/mobile-security-tools>
- ▶ 訂閱資訊保安警報
 - <https://www.hkcert.org/subscription>



Q & A