Introduce SCADA vulnerability and a little suggestion for vulnerability numbering format

Kai – Chi Chang (K.C.)

2012/11/12

Botnet@icst.org.tw

NESOKING@Gmail.com

Outline

- My Organization
- The Basic
  - CVE & OSVDB
  - SCADA
- Our Experience
- My propose
- Conclusion

My Organization

- I work for III (Institute for Information Industry)

- My department is Cyber Trust Technology Institute
  – Information Security Service Center

CVE & OSVDB

- CVE (Common Vulnerabilities and Exposures)
  - That is the most popular vulnerability database
  - It is good for searching, but the CVE number includes few information

- OSVDB
  - That is open source vulnerability database, it focuses on open source software
  - The goal of the project is to provide accurate, detailed, current and unbiased technical information on security vulnerabilities.
  - It is good for searching, but the OSVDB number includes few information

OSVDB

Timeline

Disclosure Date
2012-10-28

Description

Easy Webinar Plugin for WordPress contains a flaw that may allow an attacker to carry out an SQL injection attack. The issue is due to the get_widget.php script not properly sanitizing user-supplied input to the 'wid' parameter. This may allow an attacker to inject or manipulate SQL queries in the back-end database, allowing for the manipulation or disclosure of arbitrary data.

Classification

Location: Remote / Network Access
Attack Type: Input Manipulation
Impact: Loss of Integrity
Solution: Solution Unknown
Exploit: Exploit Unknown
Disclosure: Third-party Verified, Uncoordinated Disclosure
OSVDB: Web Related

Solution

OSVDB is not aware of a solution for this vulnerability.

Products

EasyWebinarPlugin + WATCH	Easy Webinar Plugin for WordPress + WATCH	Unspecified

References

- Exploit Database: 22300
- Vendor URL: http://www.easywebinarplugin.com/

Manual Testing Notes

```
http://[target]/wp-content/plugins/webinar_plugin/get-widget.php?wid=[SQLi]
```

Sometimes, It doesn't work

```
(.4@.9Vuln.15).7 http://sekai.hu/contact.php .15(.4@.3Windows NT EZ02--V00204 6.1 build 7601
(Unknow Windows version Web Server Edition Service Pack 1) i586.15)(.4@.9safemode-OFF.15).
:rasta!~rasta@server.sitexpression.net PRIVMSG #damai !xml /xmlrpc.php "/pnSession.php" +admin
:DaTadNs!~scan@IRCsystem-43280915.datadns.es PRIVMSG #damai :.12[.12[.9XML.12]] .9Dork :.4 "/
pnSession.php" +admin
:DaTadNs!~scan@IRCsystem-43280915.datadns.es PRIVMSG #damai :.12[.12[.9XML.12]] .13Bugz :.4 /
xmlrpc.php
```

Hacker's command

```
ystem-A8381310.gn-noc.com PRIVMSG #damai :.12[.12[.9XML.12]] .13Bugz :.4 ''/nucleus/xmlrpc/server.php''
ystem-A8381310.gn-noc.com PRIVMSG #damai :.12[.12[.9XML.12]] .3Search Engine Loading ...
ystem-7B0CF08B.azuni.net PRIVMSG #damai :.12[.12[.9XML.12]] .9Dork :.4 +pmachine
ystem-7B0CF08B.azuni.net PRIVMSG #damai :.12[.12[.9XML.12]] .13Bugz :.4 ''/nucleus/xmlrpc/server.php
```

Victim's Report

Nucleus - XML-RPC Interface

XML-RPC Interface

Introduction

Find Vulnerability on Internet

Back to the developer docs index

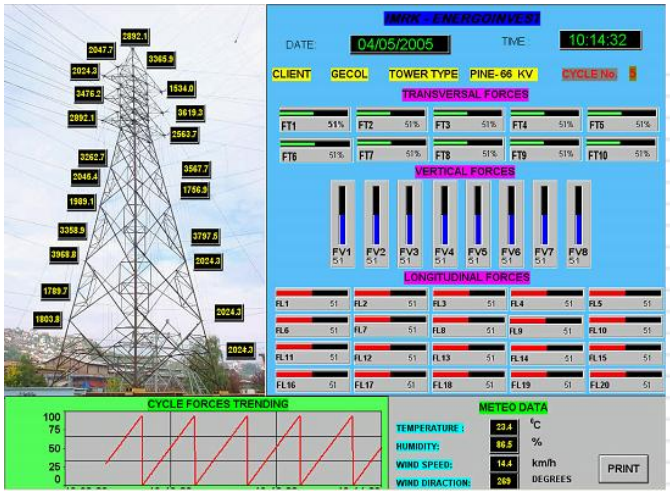
This document contains information on the XML-RPC interface that Nucleus provides, and the **error messages** it spits out. Please note that the specification of this interface might still undergo changes in the future.

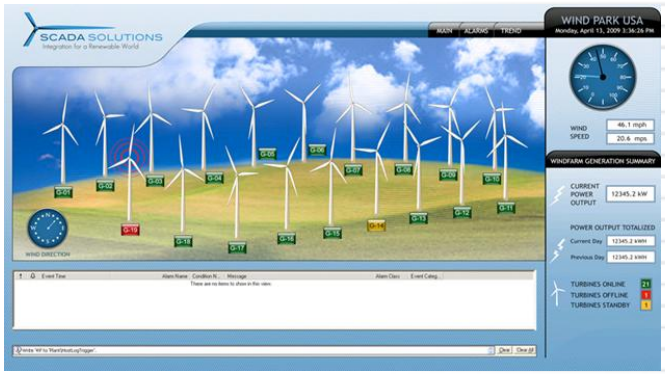
The URL for the Nucleus XML-RPC interface is:
http://www.yourserver.com/yourpath/nucleus/xmlrpc/server.php

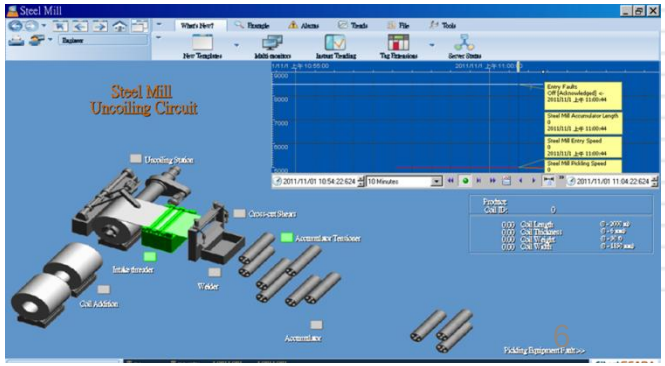
SCADA

- What is SCADA ?
  (Supervisory Control and Data Acquisition)
  - It is a part of ICS (Industrial Control System)
  - If it could monitor system and extract the data then it is SCADA

- In the different domain, it could have different functions It should has the basic unit
  - Human Machine Interface, HMI
  - Monitor System and Extract Data
  - Remote Terminal Unit, RTU
  - Programmable Logic Controller, PLC
  - Communication infrastructure



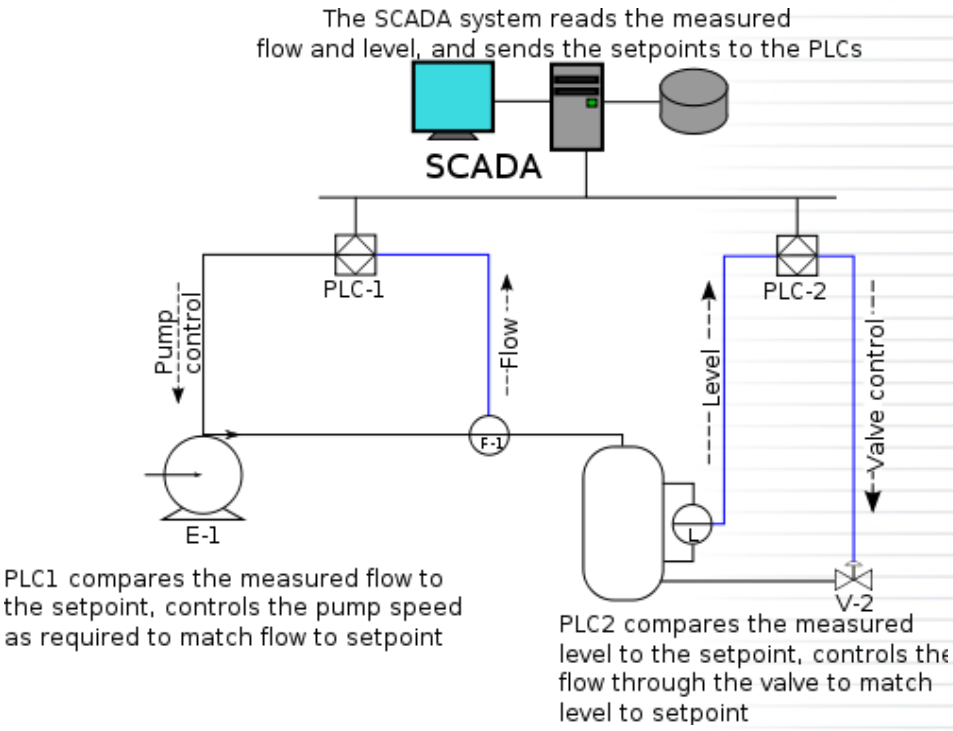




How does SCADA work?

- SCADA could Control hard ware and extract data by Computer、PLC and User Interface
  - In powerhouse, SCADA needs to collect a lot of information.
  - Those information include voltage, temperature, humidity Etc.
  - To monitor those information and record those data.
  - According to the information, SACADA could regulate voltage in the real time

Why do we need that?



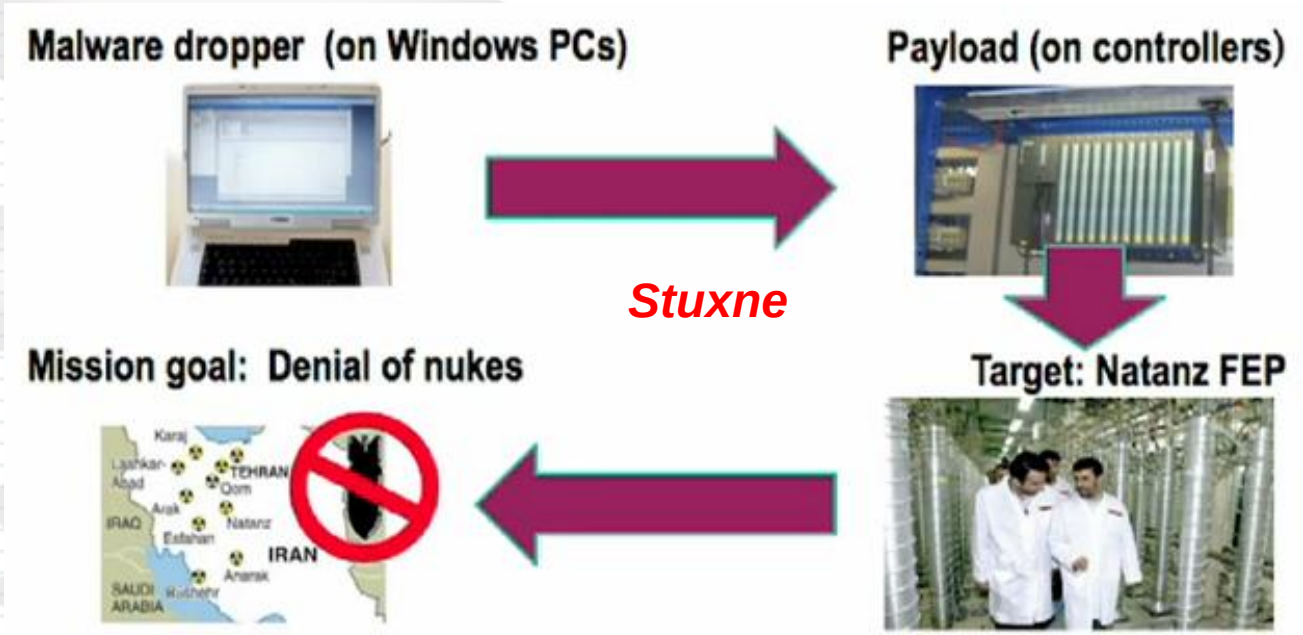
Ref.：http://en.wikipedia.org/wiki/SCADA

Only in the powerhouse?

Where can find SCADA?

Stuxnet & Duqu

- Stuxne(2010) and Duqu Worm(2011)
  - All of them, the attack target is SCADA
  - Hacker infect USB device or malicious file spread other



Ref. http://www.youtube.com/watch?v=LwCU0B6PMi0&feature=share

Our experience for revealing vulnerability

Kuang - Chun Hung (Morgan)

- Notify the CERT about 36
  - Notify ICS-CERT：26 zero day
  - Notify JPCERT/CC：9 zero day
  - Notify CERT/CC：1 zero day

- We get the 36 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、CVE-2012-3010、CVE-2012-3021、CVE-2012-3022、CVE-2012-3023、CVE-2012-3035、CVE-2012-3026

Vendor

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

Our experience for revealing vulnerability

- We can be found some acknowledgment on the ICS-CERT webside

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				

Our experience for revealing vulnerability

OSVDB: The Open Source Vulnerability Database - Mozilla Firefox

檔案 (F) 編輯 (E) 檢視 (V) 歷史 (S) 書籤 (B) 工具 (T) 說明 (H)

osvdb.org/credittees/7279-kuang-chun-hung

.:[packet storm]:. - http:··· FIRST.org / Kyoto 2012··· THN : The Hacker News Offensive Secmost ad··· android cracking Andre' M. DiMino -Sem··· 2012 Cyber Attacks Tim···

OSVDB: The Open Source Vulnerability Dat···

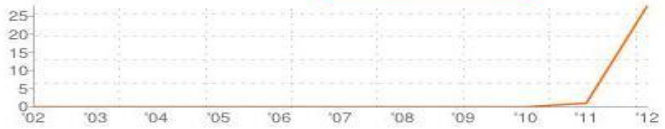
Known Contact Information:

- None at this time

Known Affiliations:

- Information and Communication Security Technology Center *(as of 2011-12-2*

Vulnerability Disclosures By Kuang-Chun Hung Over Time



Disclosed Vulnerabilities (29):

Disc. Date	OSVDB ID	CVEID	Title
2012-10-15	86257	2012-3026	General Electric (GE) Intelligent Platforms Proficy Real-Time Information Portal Unspecified Overflow (2012-3026)
2012-10-15	86258	2012-3010	General Electric (GE) Intelligent Platforms Proficy Real-Time Information Portal Unspecified Overflow (2012-3010)
2012-10-15	86259	2012-3021	General Electric (GE) Intelligent Platforms Proficy Real-Time Information Portal Unspecified Overflow (2012-3021)
2012-09-28	85822	2012-3035	DeltaV Malformed String Parsing Remote Overflow DoS
2012-05-16	82014	2012-1818	DeltaV Multiple Product Unspecified ActiveX Arbitrary File Overwrite
2012-05-16	82011	2012-1815	DeltaV Multiple Product Unspecified SQL Injection
2012-05-16	82012	2012-1816	DeltaV Multiple Product PORTSERV.exe Packet Parsing Remote DoS
2012-05-16	82013	2012-1817	DeltaV Multiple Product Project File Handling Remote Overflow
2012-05-16	81996	2012-1814	DeltaV Multiple Product Unspecified XSS
2012-02-17	79407	2012-0223	7-Technologies TERMIS Unspecified Path Subversion Arbitrary DLL Injection Code Execution
2012-02-17	79408	2012-0224	7-Technologies AQUIS Unspecified Path Subversion Arbitrary DLL Injection Code Execution
2012-02-16	79563	2012-0234 2012-1234	Advantech/Broadwin WebAccess Unspecified SQL Injection (2012-0234)
2012-02-16	79570	2012-0235 2012-1235	Advantech/Broadwin WebAccess Unspecified CSRF
2012-02-16	79562	2011-4521	Advantech/Broadwin WebAccess Unspecified SQL Injection (2011-4521)
2012-02-16	79566	2012-0233	Advantech/Broadwin WebAccess Unspecified XSS
2012-02-16	79569	2012-0236	Advantech/Broadwin WebAccess Unspecified Information Disclosure
2012-02-16	79574	2012-0237	Advantech/Broadwin WebAccess Unauthorized Date/Time Syncing Modification
2012-02-16	79575	2012-0238	Advantech/Broadwin WebAccess opcImg.asp Remote Overflow
2012-02-16	79577	2012-0239	Advantech/Broadwin WebAccess uaddUpAdmin.asp Unauthorized Admin Password Manipulation
2012-02-16	79578	2012-0240	Advantech/Broadwin WebAccess GbScriptAddUp.asp Authentication Function Remote Code Execution
2012-02-16	79576	2011-4524	Advantech/Broadwin WebAccess Unspecified Overflow (2011-4524)
2012-02-16	79585	2011-4526	Advantech/Broadwin WebAccess Unspecified ActiveX Overflow
2012-02-16	79586	2011-4525	Advantech/Broadwin WebAccess Arbitrary File Write Remote Code Execution
2012-02-16	79567	2011-4522	Advantech/Broadwin WebAccess bwerrdn.asp Unspecified XSS
2012-02-16	79568	2011-4523	Advantech/Broadwin WebAccess bwview.asp Unspecified XSS
2012-02-16	79587	2012-0243	Advantech/Broadwin WebAccess bwocxrun.ocx Overflow Arbitrary File Creation Code Execution
2012-02-16	79565	2012-0244	Advantech/Broadwin WebAccess Unspecified SQL Injection (2012-0244)
2012-01-16	78328	2011-4053	7-Technologies Interactive Graphical SCADA System Path Subversion Arbitrary DLL Injection Code Execution
2011-12-21	78233	2012-0309	Cogent DataHub Unspecified XSS

That is CVE number

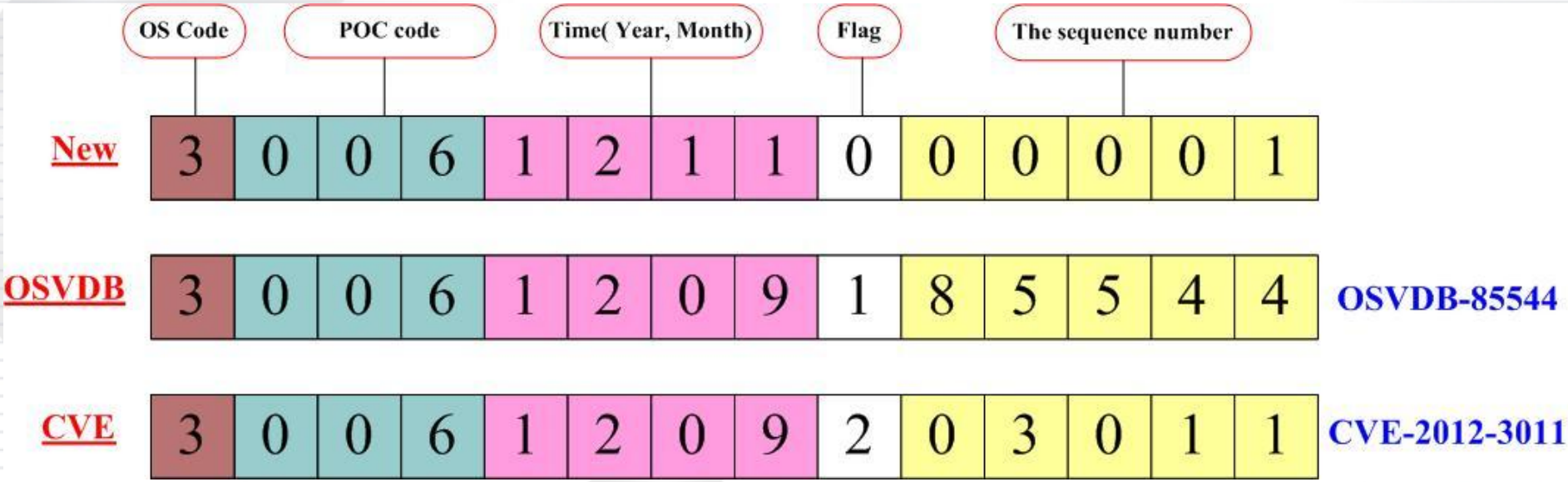
- That is the CVE number
  - CVE-2011-1914、CVE-2011-3330、CVE-2011-3996、CVE-2011-4033、CVE-2011-4034、CVE-2011-4035、CVE-2011-4036、CVE-2011-4043、CVE-2011-4053、CVE-2011-4055、CVE-2011-4056、CVE-2011-4057、CVE-2011-4521、CVE-2011-4522、CVE-2011-4523、CVE-2011-4524、CVE-2011-4525、CVE-2011-4526、CVE-2011-4533、CVE-2011-4534、CVE-2011-4870、CVE-2012-0223、CVE-2012-0224、CVE-2012-0309、CVE-2012-0310、CVE-2012-1814、CVE-2012-1815、CVE-2012-1816、CVE-2012-1817、CVE-2012-1818、CVE-2012-3010、CVE-2012-3021、CVE-2012-3022、CVE-2012-3023、CVE-2012-3035、CVE-2012-3026
- May I have a easier way to understand what it means?

My propose

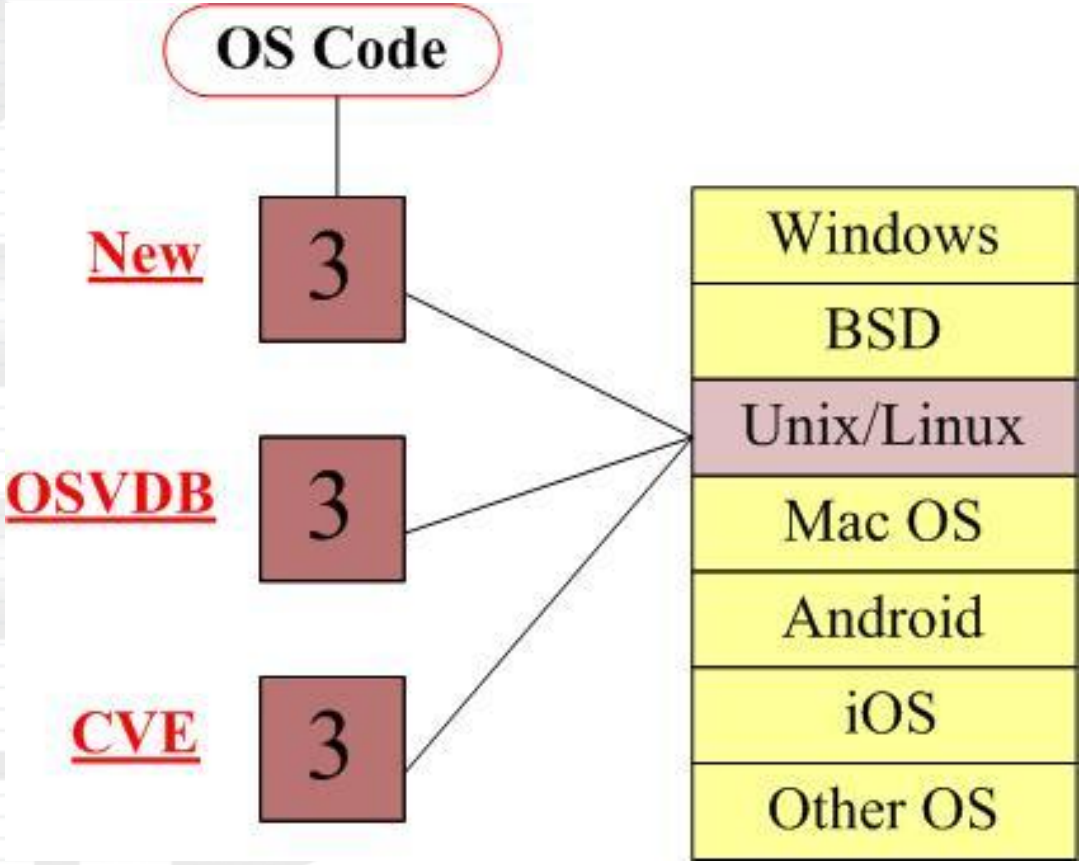
- The idea of vulnerability numbering format
  - It is possible to have a easy way to know the meaning of the number
    - ◎ If it is possible, It should have the vulnerability's OS、the attack type of POC and time
  - If it is possibe, base on the CVE and OSVDB is better
    - ◎ If we do that, all of vulnerability could be integrated

- Any Cert in FiRST can reveal vulnerabilities
  - We may have ability to find the vulnerabilities, and we want to notify other organizations (It takes a lot of time)

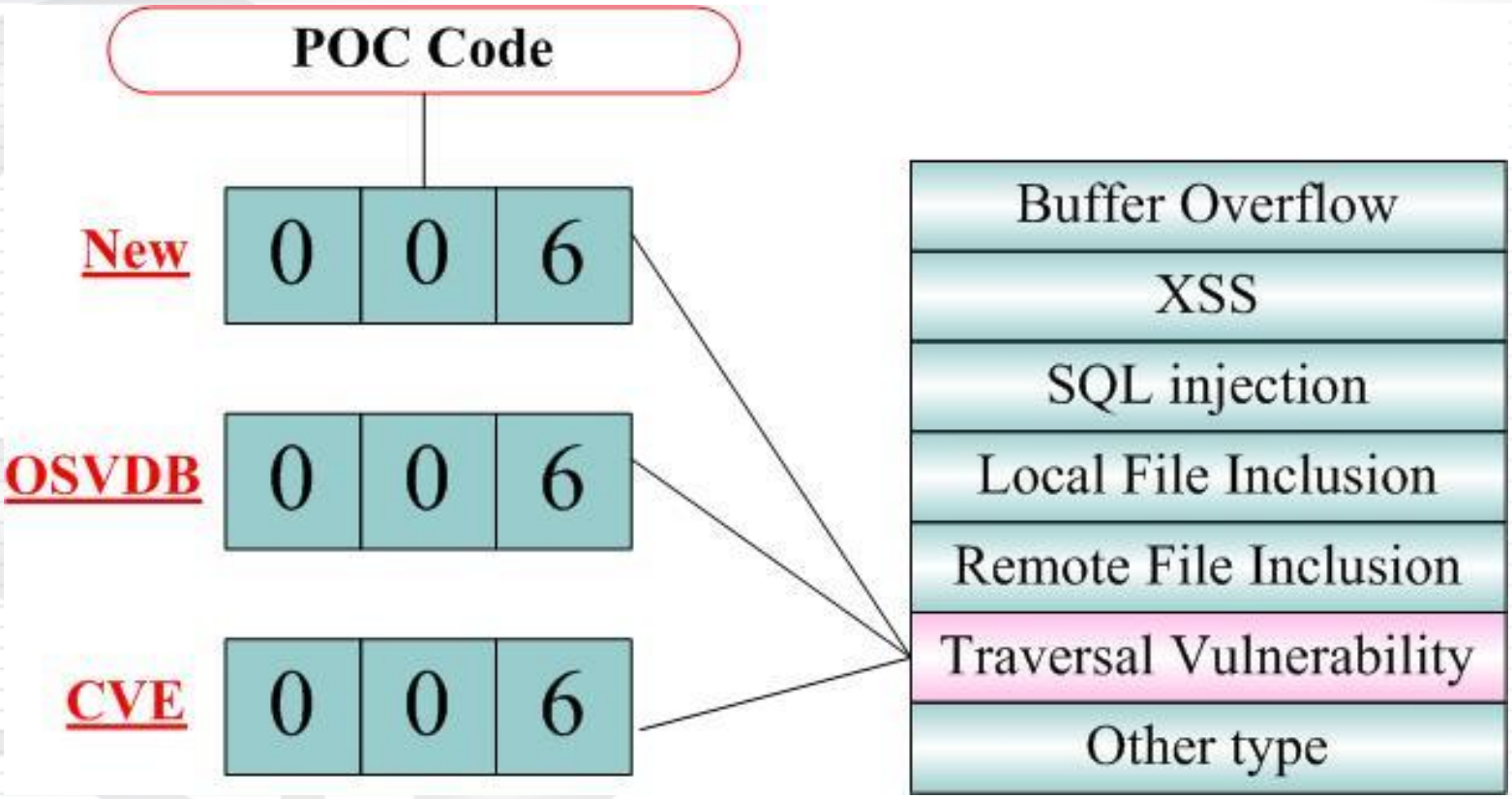
The Idea of vulnerability numbering format



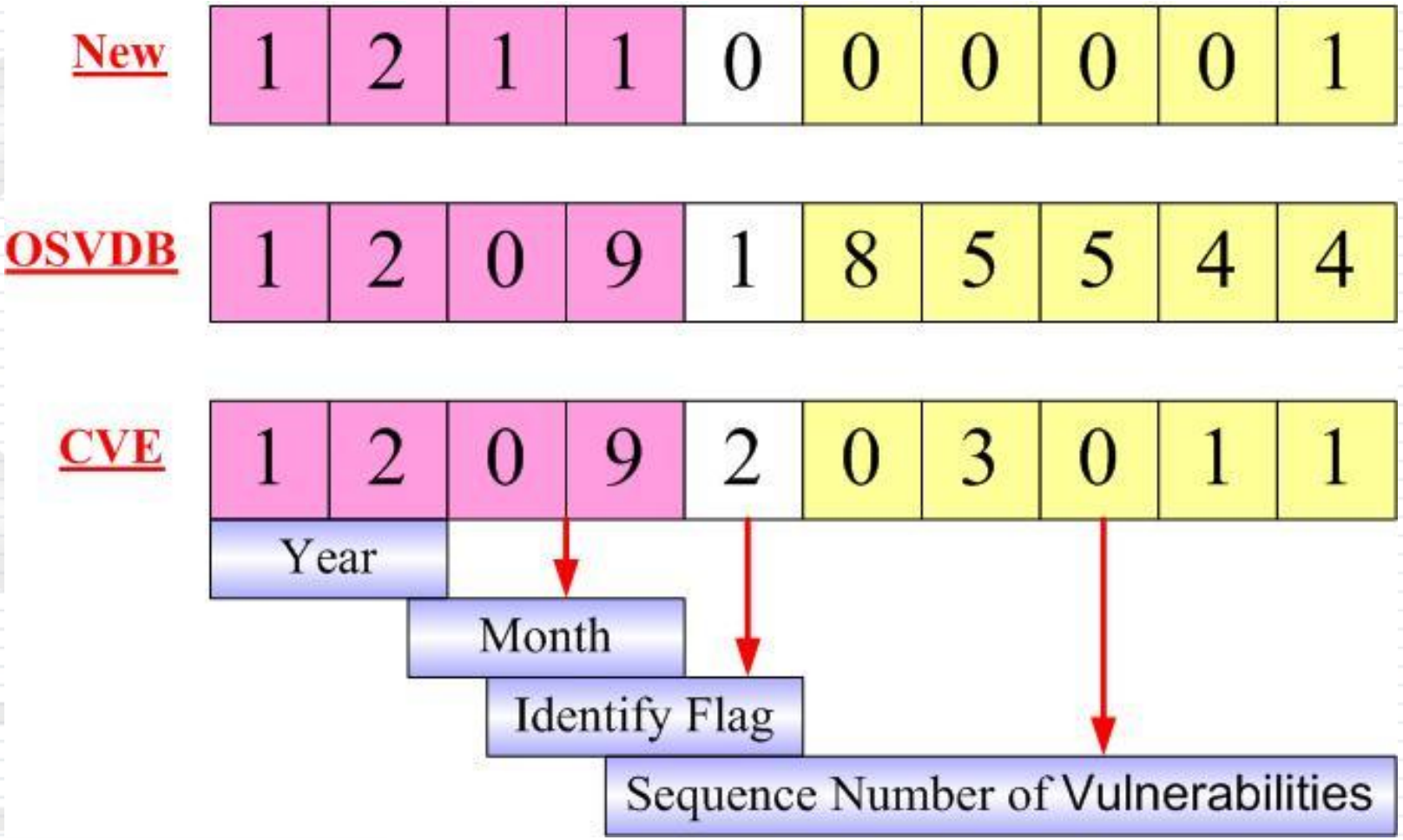
The Idea of vulnerability numbering format



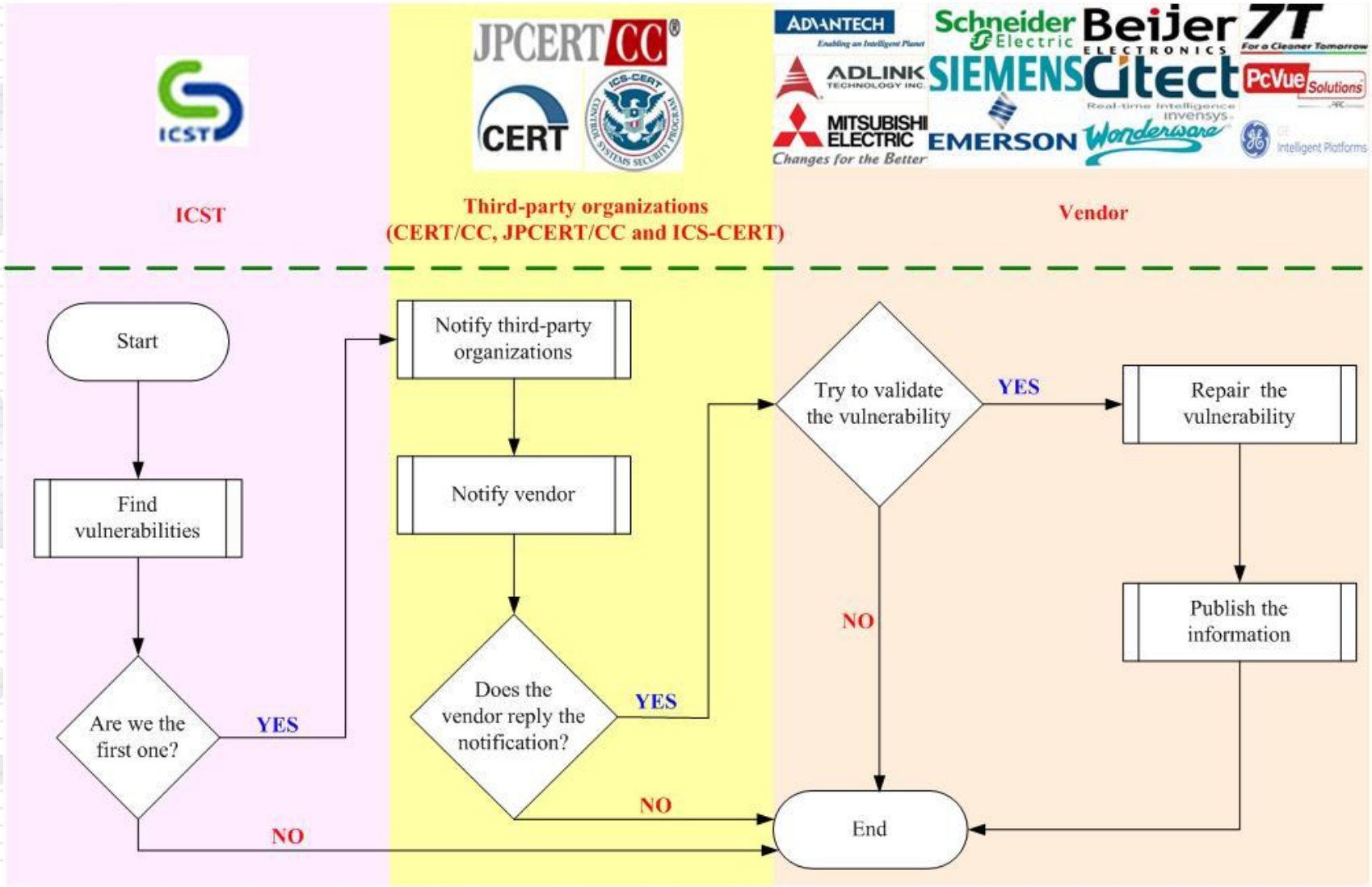
The Idea of vulnerability numbering format



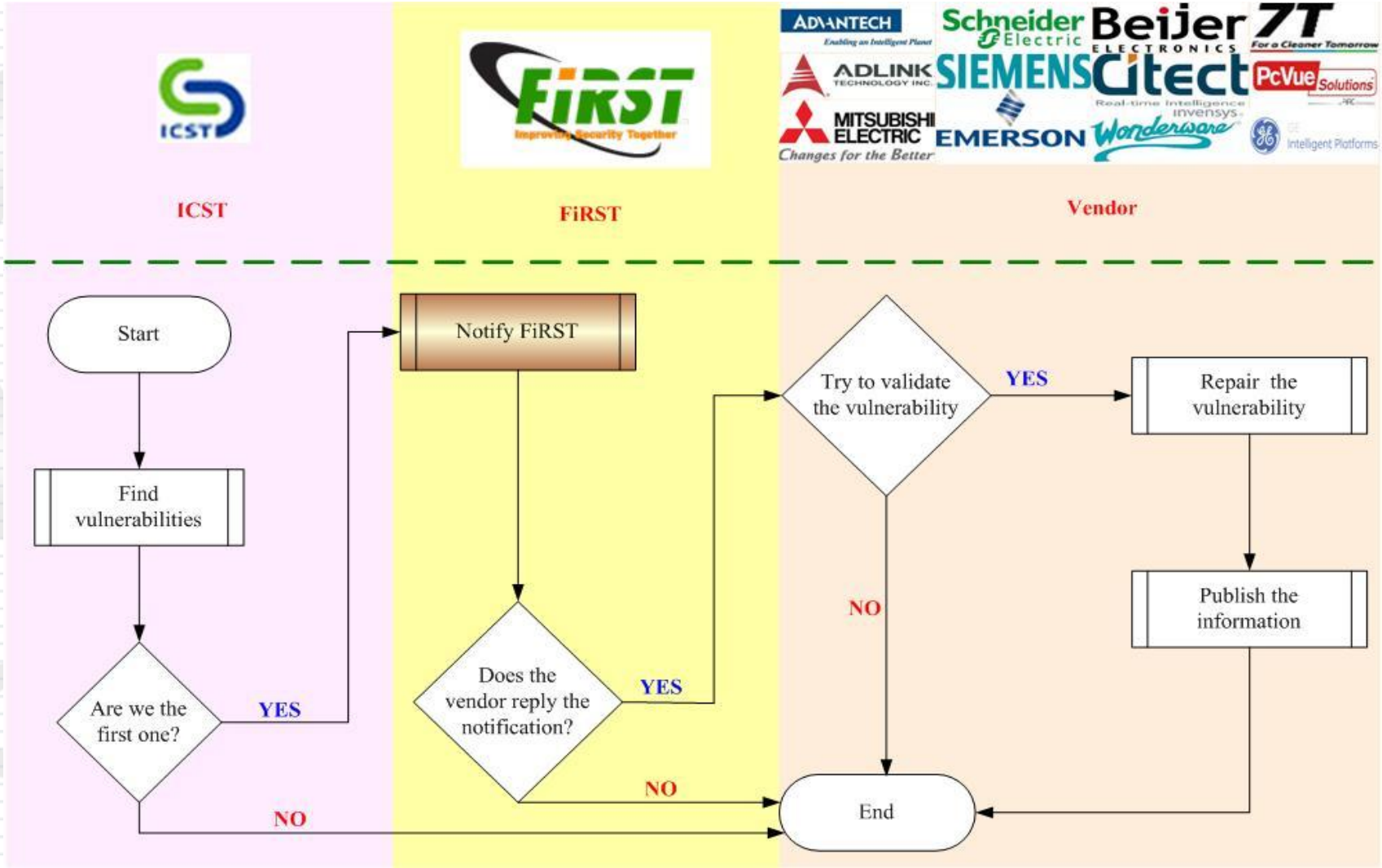
The Idea of vulnerability numbering format



Any Cert in first can reveal vulnerabilities



Any Cert in first can reveal vulnerabilities



Conclusion

- The SCADA issue is more and more important.
  - We will still use fuzzing technology to find more vulnerabilities in the future.
- CVE and OSVDB are most popular vulnerability database, but the number is difficult to identify some information.
- Using the new format, it could identify
  - Which kind of OS
  - Which attack type of POC
  - And, it base on CVE and OSVDB number
- At last, if any Cert reveal vulnerabilities to FiRST, It would shorten the time of notification

Thank you for your kind attention

Q&A