Open Source and CSIRT
- What can we do?-

Presented by:

Yoshiki Sugiura, CSIRT Evangelist
Shin Adachi, CISSP, CISM, CISA, PMP

FIRST OF ALL

Congratulations HITCON on your 10th Anniversary!

祝10週年 台灣駭客年會!
This presentation ONLY reflects personal views and opinions of the presenters, NOT presenters’ affiliations IN ANY WAY, including but not limited to their employers, customers, associations, and so on.

---

PRESENTED BY

- CSIRT Evangelist
  - JPCERT/CC from 1998 to 2002
  - NTT-CERT, Intelli-CSIRT
  - Steering committee of Nippon CSIRT Association.
- GNU/Linux, Emacs
- Guest researcher of Meiji Univ.
  - Team building
  - Theory of management and Social psychology
AND..

• Silicon Valley InfoSec Geek
  • FIRST Education Committee Chair
  • CISSP, CISM, CISA, and PMP
  • NTT-CERT
  • ENISA Expert/Working Groups
  • Info Security consultant

• Contributed to:
  • NIST SP 500-291 and *293
  • Liberty Alliance Presence Services, eGov Profile v1, IAF, Strong Authentication etc.
  • ITU-T: NGN Security and IdM

MISSING HIM, WHO CAN'T COME TODAY..

• IT gadget otaku
• Photographer
• Consultant

• vi/emacs
• grep/sed/awk
• Debian/Linux
• OS X

• Father
Root cause of most cyber security incidents
CASE #1- WORLDCUP 2014

Source: https://twitter.com/apbarros/status/481157619261116416/photo/1

Source: https://twitter.com/apbarros/status/481157619261116416/photo/1
SOFTWARE VULNERABILITIES

Source: 25 Years of Vulnerabilities: 1988-2012
by sourcefire

![Graph showing software vulnerabilities over time.]

QUIZ

How many Apache related vulnerabilities were published in 2012 and 2013?

2014 (as of July 31)  
67

2013:  
135

2012:  
129

CASE #2: CVE-2013-1966

Vulnerability

- in Apache Struts 2 before version 2.3.14.1
- allows remote attackers
- to execute arbitrary OGNL code
- via a CRAFTED request that is NOT PROPERLY HANDLED when using the includeParams attribute in
  i. a URL, or
  ii. a tag.

Reference: http://struts.apache.org/development/2.x/docs/s2-013.html
What is Struts?

- Open source web application Framework
- Based on MVC architecture
- Struts 2

Vulnerability

- in Apache Struts 2 before version 2.3.14.1
- allows remote attackers
- to execute arbitrary OGNL code
- via a CRAFTED request that is NOT PROPERLY HANDLED when using the includeParams attribute in
  i. a URL, or
  ii. a tag.

Reference: http://struts.apache.org/development/2.x/docs/s2-013.html
More serious in Japan than any other places

• Not yet sure why 😐

• Many websites in Japan compromised

• Such sites spread malware to users through drive by download

• Needed to apply the patch as soon as it was released…
  
  • when Japan was in big holiday week on April~May.

• Many sites are still suspected vulnerable…😢
What are the problems?

1. Developers
   - Lack of Secure Development
   - Lack of Secure Coding

CASE #2: CVE-2013-1966

What are the problems?

2. Users ~_~;;
   - Didn’t care of patches 😞
     - No Patch management in the worst cases
   - Did not consider security enough, or at all 😞
   - Even Struts 1s were still running after its support expired… (Windows XP, you are not alone. 😱)
What are the problems?

3. Vendors, or System Integrators
   - Some vendors did not have contractual obligations to fix vulnerabilities.
   - Some of them even not familiar enough with patching or patch management.
SECURITY ISSUES AROUND OPEN SOURCE


Awareness test

COMMERCIAL BETTER?

26
OPEN SOURCE SOFTWARE AS “FREE” SOFTWARE

• Do it ourselves at our own risk.
• We have all or majority of controls.

It’s “Free”
Back to the root
“Have fun!”

AGENDA

Issues on OSS
Roles of CSIRT
OSS Security Tools
WHAT CAN CSIRTS DO FOR OPEN SOURCE?

“An ounce of prevention equals a pound of cure.”
By Benjamin Franklin

Patch and Vulnerability Group (PVG)
- Manage patch and Vulnerability
- Zero-day -> Mitigation

Creating a Patch and Vulnerability Management Program

Recommendations of the National Institute of Standards and Technology (NIST)

CSIRT AND COMMUNITIES

- Vulnerability information
- Best practices
- Knowledge

EARLY WARNING PARTNERSHIP FOR INFORMATION SECURITY IN JAPAN

http://www.jpcert.or.jp/english/te/project.html
AGENDA

- Issues on OSS
- Roles of CSIRT
- OSS Security Tools

OSS SECURITY TOOLS

- Kali Linux
- Pen
- Metasploit
- Skipfish
Many useful tools are already available.
  - Commercial level software are also there
  - Attacker are also using those tools…
  - Know your enemy?

OSS security tool community
  - different motivation from other OSS softs
  - useful to share knowledge and information
  - more security experts

OSS SECURITY TOOLS

- for admins/developers
  - IDS/IPS, WAF, Firewalls,
  - Penetration testing, code testing

- for end users
  - data encryption & signing
  - data rescue

- for security professionals
  - security analysis tools
  - digital forensic, malware analysis, pentest
REFERENCES OF OSS SECURITY TOOLS

Top 125 Network Security Tools
http://sectools.org/

Probably best free security list
https://www.techsupportalert.com/content/probably-best-free-security-list-world.htm

SHARE SECURITY TOOLS, KNOWLEDGE, AND EXPERIENCES

• Beginners
  • I don’t know which one are good.
  • I don’t know how to use them
  • I don’t know how to Google them.
  • I don’t know how to learn them.

• Seniors- those more experienced
  • I like these ones best among others.
  • I know how to use them.
  • “Use the Source, Luke”, in addition to Just Googling them to know!
  • Do it to learn it
WHY DON’T WE HELP?

• Security requires a lot of hands-ons.
• Beginners need Seniors.
• Bring up new Jedi’s for future internet security.
• Expect young generation do more than we are doing.

CONCLUSION
MORE CONSIDERATIONS

- Best practices using Open Source Software
- User Vulnerability Educations
- Secure Development and Secure Coding
- OSS Security Tools repository and how to use them (Hands on)

QUESTIONS?
SPECIAL THANKS TO

Daphne Hsu
PeiKan Tsung
Kris Lin
All other HITCON Staff
AND
All of you here now!

ACKNOWLEDGEMENT

Mr. Keisuke Kamata
Mr. Tomoyuki Kuroda, OSS Forum Japan
Mr. Masahito Yamaga
Ms. Natsuko Inui, CDI-CIRT
Mr. Hitoshi Endo, NTT-CERT
Mr. Ikuya Hayashi, NTT-CERT