CSA APAC cloud security alliance®
ASIA PACIFIC REGION

雲漏洞報告小組計劃

Mickey Law
研究分析員, 亞太區
雲安全聯盟

cloudsecurityalliance.org facebook.com/csaapac1
Cloud Security Alliance cloudsa_apac csa_china

網絡安全？

Fixing Vulnerabilities

Average fix time for website vulnerabilities:

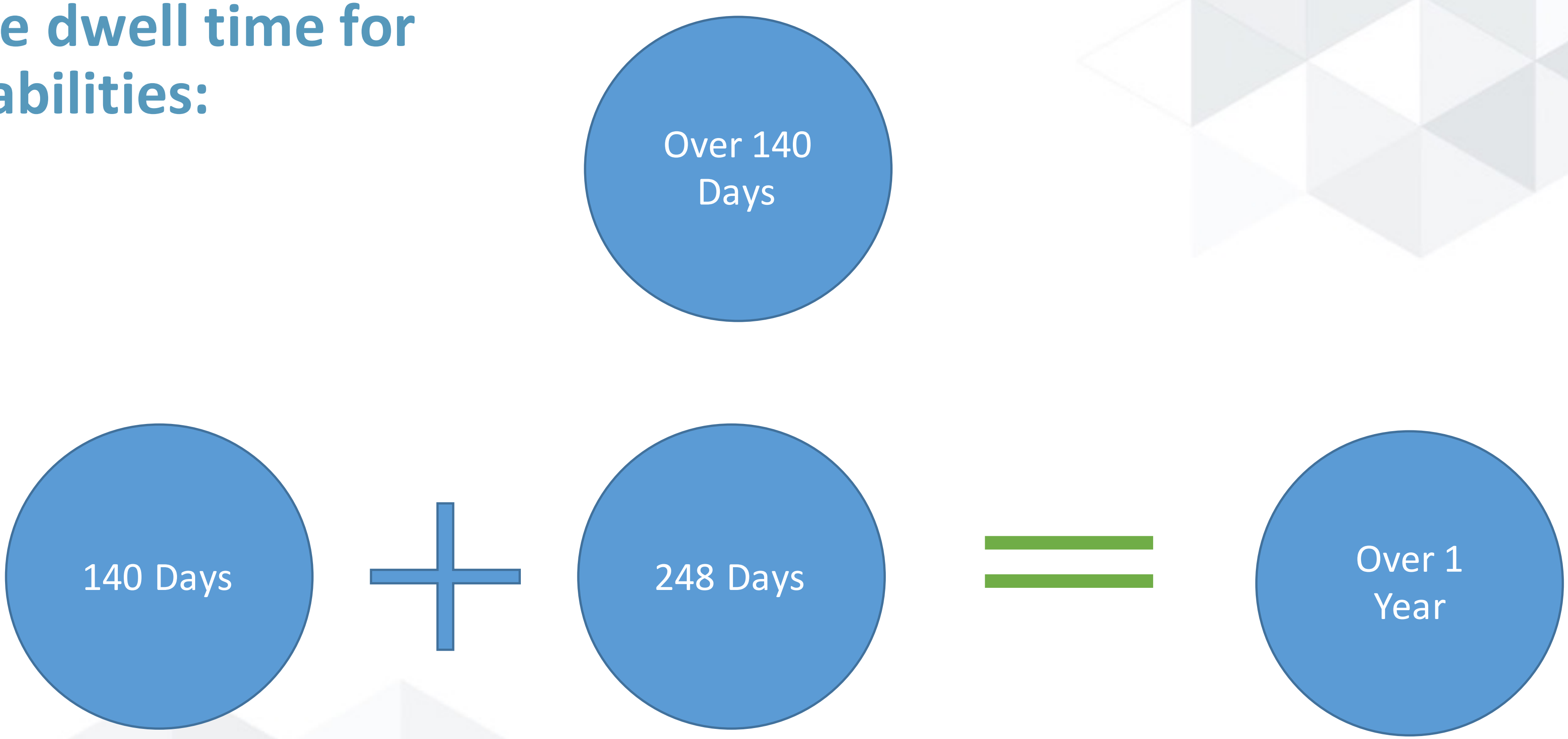
150 – 180 Days

Average fix time for software vulnerabilities:

248 Days

Fixing Vulnerabilities

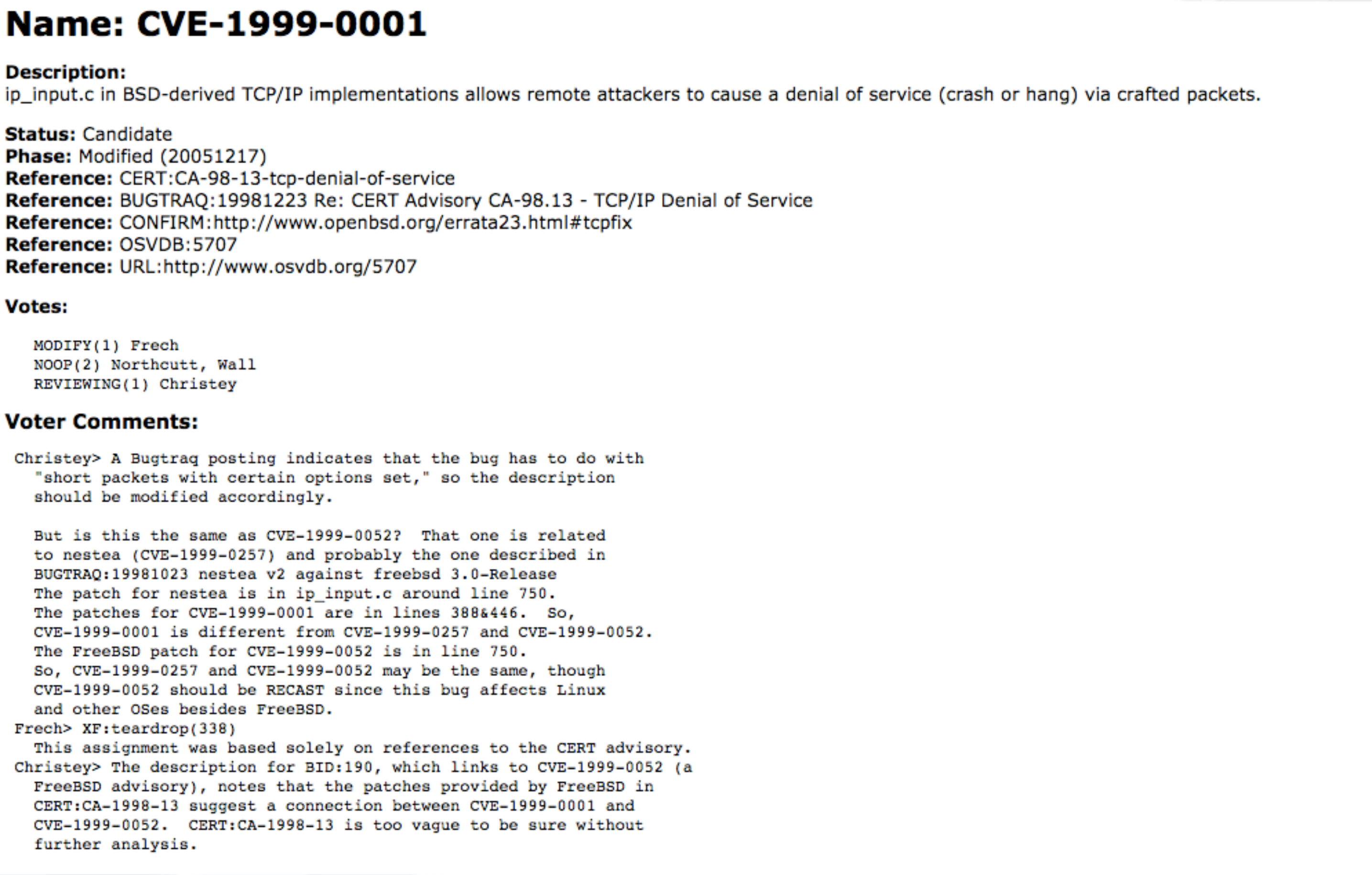
Average dwell time for vulnerabilities:



Over 140 Days

140 Days + 248 Days = Over 1 Year

Common Vulnerabilities and Exposures (CVE)



Name: CVE-1999-0001

Description:
ip_input.c in BSD-derived TCP/IP implementations allows remote attackers to cause a denial of service (crash or hang) via crafted packets.

Status: Candidate
Phase: Modified (20051217)
Reference: CERT:CA-98-13-tcp-denial-of-service
Reference: BUGTRAQ:19981223 Re: CERT Advisory CA-98.13 - TCP/IP Denial of Service
Reference: CONFIRM:http://www.openbsd.org/errata23.html#tcpfix
Reference: OSVDB:5707
Reference: URL:http://www.osvdb.org/5707

Votes:

```
   MODIFY(1) Frech
   NOOP(2) Northcutt, Wall
   REVIEWING(1) Christey
```

Voter Comments:

```
 Christey> A Bugtraq posting indicates that the bug has to do with
   "short packets with certain options set," so the description
   should be modified accordingly.

   But is this the same as CVE-1999-0052?  That one is related
   to nestea (CVE-1999-0257) and probably the one described in
   BUGTRAQ:19981023 nestea v2 against freebsd 3.0-Release
   The patch for nestea is in ip_input.c around line 750.
   The patches for CVE-1999-0001 are in lines 388&446.  So,
   CVE-1999-0001 is different from CVE-1999-0257 and CVE-1999-0052.
   The FreeBSD patch for CVE-1999-0052 is in line 750.
   So, CVE-1999-0257 and CVE-1999-0052 may be the same, though
   CVE-1999-0052 should be RECAST since this bug affects Linux
   and other OSes besides FreeBSD.
 Frech> XF:teardrop(338)
   This assignment was based solely on references to the CERT advisory.
 Christey> The description for BID:190, which links to CVE-1999-0052 (a
   FreeBSD advisory), notes that the patches provided by FreeBSD in
   CERT:CA-1998-13 suggest a connection between CVE-1999-0001 and
   CVE-1999-0052.  CERT:CA-1998-13 is too vague to be sure without
   further analysis.
```

Common Vulnerabilities and Exposures (CVE)

• Manual Process	• 手動流程
• Anyone can contribute	• 任何人都可以做出貢獻
• Long verification time	• 長驗證時間
• Too late to fix already	• 修復也於事無補了

How to be more Active?

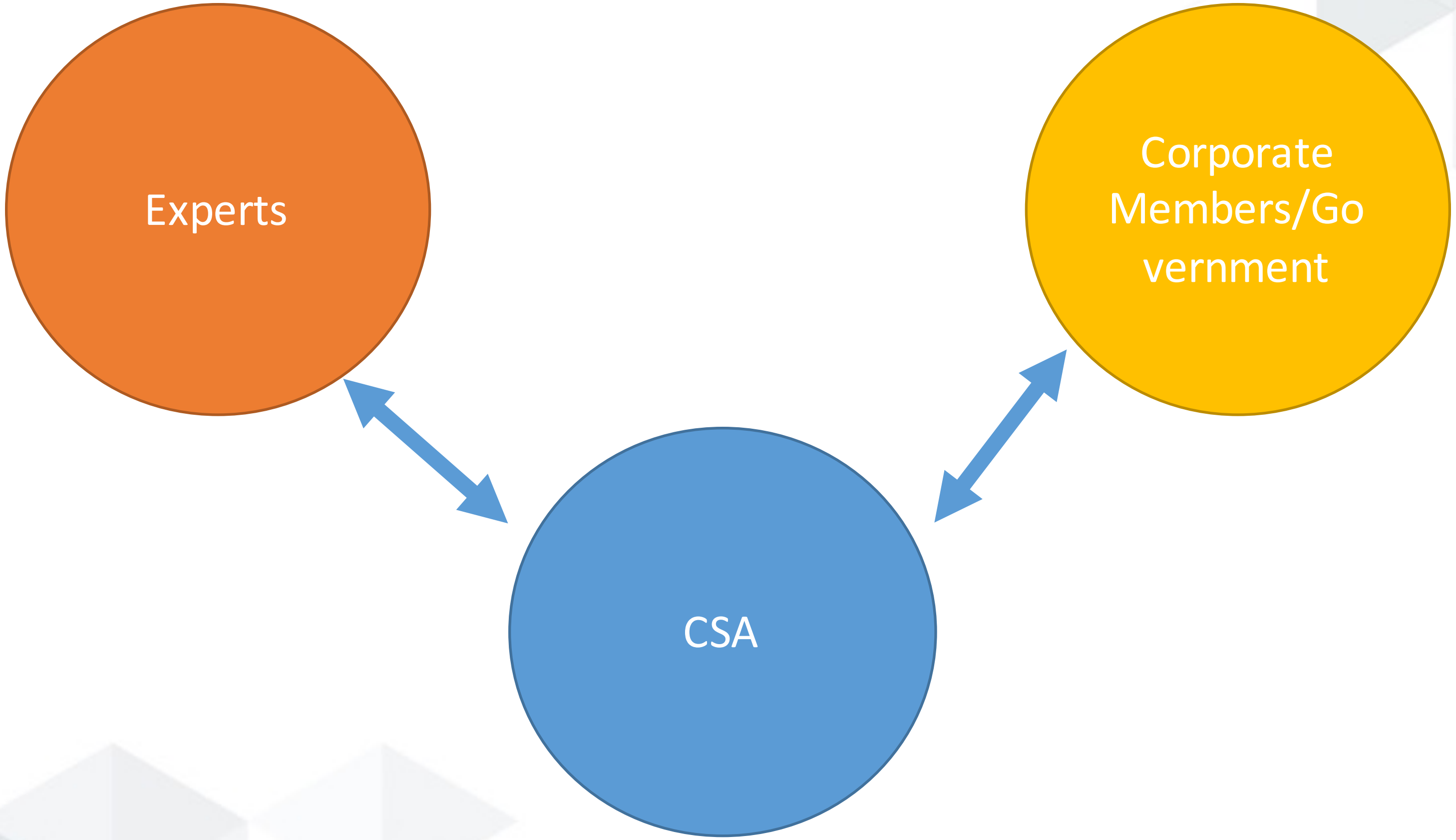
CSA Characteristics：

- Corporate Members
- Solution Providers
- Enterprise Costumers
- Education Institutes
- Analysts
- Trusted Individual Members
- Government

CSA的特色：

- 企業會員
- 服務供應商
- 企業用戶
- 教育學院
- 研究員
- 可信的個人會員
- 政府

Cloud Vulnerability Reporting Framework



Objectives

- Automate the verification process
- Reward actively participate “Vulnerabilities Reporters”
- Protect the users by not reviling the vulnerabilities to the public

- Reduce the risk and security threats that organizations and individuals expose themselves to by having vulnerabilities in their information system

Join Us

- **You are a researcher**
- Help us to identify vulnerabilities!

- **You are an enterprise/government?**
- Join us to see what vulnerabilities exist in your Cloud related products/system.

- **Comments Welcome!**

Contact Us

General inquiries:

csa-apac-info@cloudsecurityalliance.org

Research information:

csa-apac-research@cloudsecurityalliance.org

Facebook: csaapac1

Twitter: @cloudsa_apac

LinkedIn: Cloud Security Alliance

Thank you!

Any Questions?