# Towards the Detection of Inconsistencies in Public Security Vulnerability Reports

Ying Dong, Wenbo Guo, Yueqi Chen, Xinyu Xing,
Yuqing Zhang, Gang Wang

Presenter: 欧国亮

# Challenges Faced by Security Operations Engineers

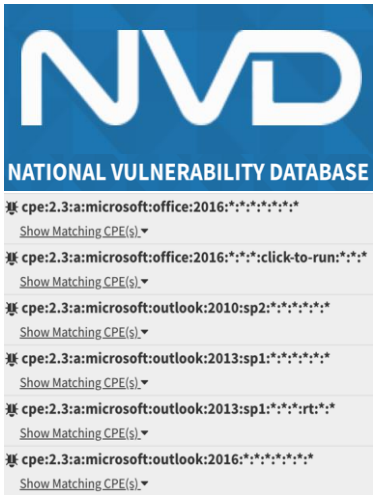
1. Keep an eye on new vulnerabilities that affect their systems
2. Patch vulnerable softwares as soon as possible

NVD
NATIONAL VULNERABILITY DATABASE

CVE®
Common Vulnerabilities and Exposures


# Inconsistent Information → Confusion

A New Vulnerability (CVE-2018-0852) is Exposed




**Microsoft outlook 2007 SP3** - NOT listed.


| Description |
| --- |
| Microsoft Outlook 2007 SP3 Microsoft Outlook 2010 SP2, Microsoft Outlook 2013 SP1 and RT SP1, Microsoft Outlook 2016, and Microsoft Office 2016 Click-to-Run (C2R) allow a remote code execution vulnerability, due to how Outlook handles objects in memory, aka "Microsoft Office Memory Corruption Vulnerability". This CVE is unique from CVE-2018-0851. |

**Microsoft outlook 2007 SP3** - listed.

# Research Problems

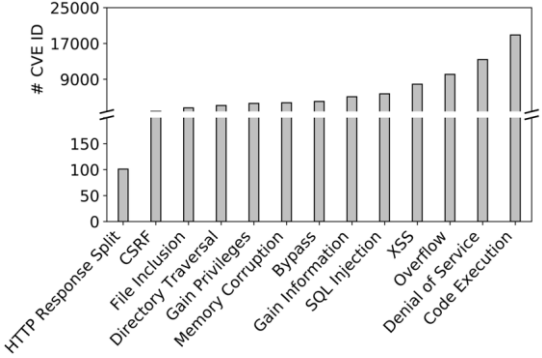
1. Is inconsistency issue prevalent?
2. What are the characteristics of inconsistent info?
3. Reasons for inconsistency?
4. Security implications of inconsistency?

# Measuring Inconsistency of Vuln. Reports

1999 - 2018

Over 20 years

Across websites




of 13 categories

# In This Paper:

Part I: VIEM - an automatic system

extract vulnerable software name and versions

Part II: Large-scale Measurement

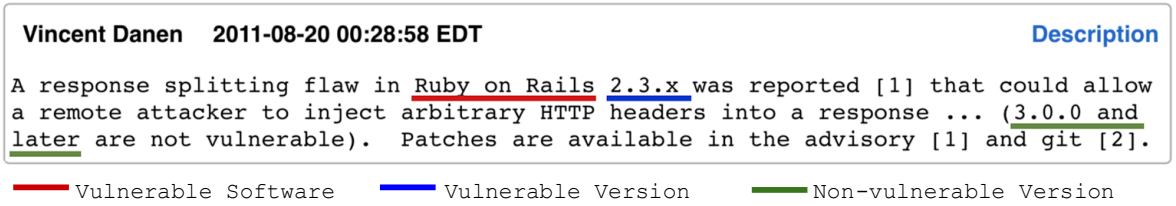
quantify inconsistency and interesting findings

# Traditional NLP Tools Don't Work Well (Validated)

1. Dictionary-based method (CNLL '06, EMNLP '13)
2. Pre-defined rules (SIGSOFT '12, CCS '17, FSE '17)
3. Regular-expression based technique (CCS '17, FSE '17)
4. Techniques handling single entity (ISESE '14, CCS '17, FSE '17)
5. Semfuzz (CCS '17)

**Reason:** Unique characteristics of vulnerability reports

# Why This Is Hard




1. Previously unseen vulnerable softwares (Ruby on Rails)
   -> Dictionary-based ✘
2. Both vulnerable (2.3.x) and non-vulnerable versions (3.0.0 and later) exist
   -> Pre-defined rules ✘
3. Reports are highly unstructured
   -> Regular-expression based ✘

# Why This Is Hard (cont.)

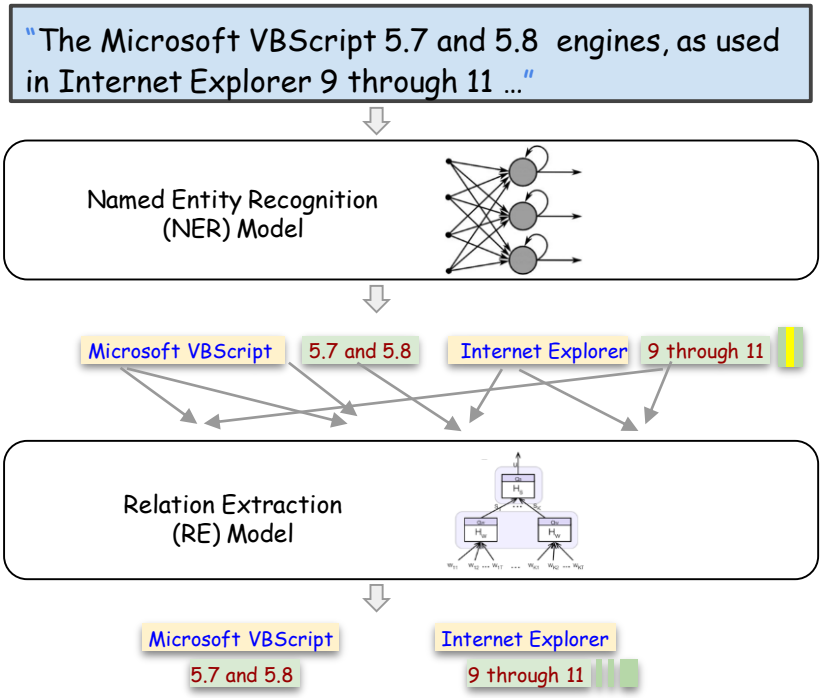
In Windows Vista SP2 and Windows Server 2008 SP2, the Windows font library in .NET Framework 3.0 SP2, 3.5, 3.5.1, 4, 4.5, 4.5.1, 4.5.2, and 4.6; Skype for Business 2016; Lync 2010; Lync 2013 SP1; and Silverlight 5 allows remote attackers to execute arbitrary code via a crafted embedded font, aka "Graphics Memory Corruption Vulnerability."

Publish Date : 2015-12-09 Last Update Date : 2017-09-12

Vulnerable Software — Vulnerable Version

4. Multiple interested entities
   -> Existing tools handling single entity ✘
5. Diverse vulnerability types
   -> Tools for certain vulnerability types (e.g., recall < 40%) ✘

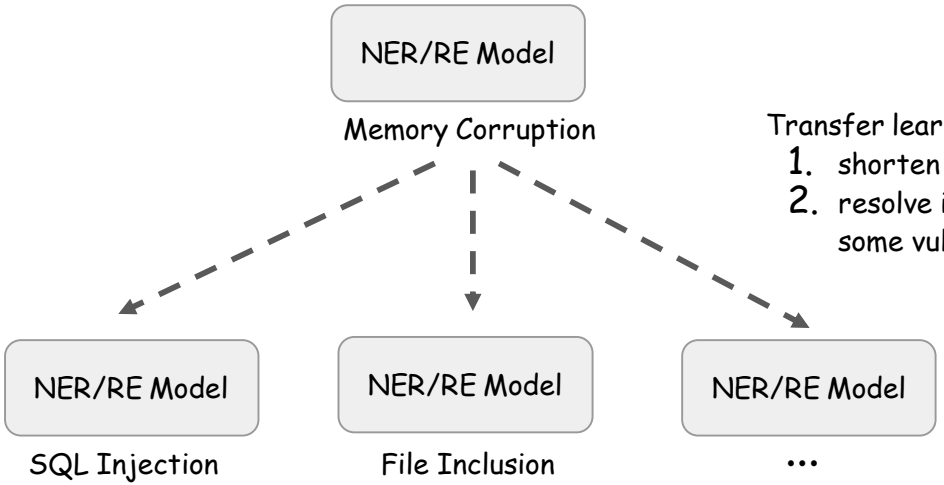
# VIEM - NER/RE Model




1. Bi-directional RNN
2. word/character embedding
3. Gazetteer

1. One-hot encoding
2. Hierarchical Attention-Network

# VIEM - Transfer Learning




Transfer learning to

1. shorten training cycle
2. resolve inadequate training data of some vulnerability categories

# VIEM - Dataset

| Dataset | Vulnerability Reports | Structured Reports | | Unstructured Reports | | |
|---|---|---|---|---|---|---|
| | | SecTracker | SecFocus | ExploitDB | Openwall | SecF Forum |
| All | 70,569 | 7,320 | 38,492 | 9,329 | 5,324 | 10,194 |
| G-truth | 1,974 | 0 | 0 | 785 | 520 | 669 |

1. Over past 20 years (1999-2018)
2. 5 representative vulnerability report websites
3. Manually labelled G-truth dataset for evaluating VIEM

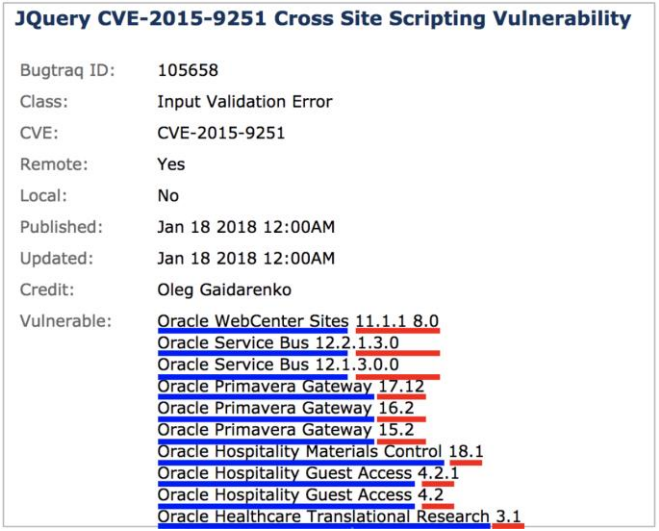
# VIEM - Dataset

```
#!/usr/bin/python
##############################################################################
#
# SmarterMail Web Server 5.0 DoS exploit
# Tested on version 5.0.2999, OS: Windows XPSP2 English
# Tested with GET,HEAD,PUT,POST,TRACE
#
# Bug discovered by Matteo Memelli aka ryujin
# http://www.gray-world.net http://www.be4mind.com
#
##############################################################################
#
# bt ~ # ./smartermail_dos.py -H 192.168.1.245 -P 9998
# [+] Connecting to 192.168.1.245 on port 9998
# [+] Starting DoS attack, it can take some minutes...
# [+] Evil buf sent!
# [+] Now we must wait for a connection reset to crash the server...
# [+] Server Di3d:  Connection reset by peer
# [+] The attack took 113 secs
#
##############################################################################

from socket import *
from optparse import OptionParser
import sys, time
```

ExploitDB

# VIEM - Dataset



**JQuery CVE-2015-9251 Cross Site Scripting Vulnerability**

| | |
|---|---|
| Bugtraq ID: | 105658 |
| Class: | Input Validation Error |
| CVE: | CVE-2015-9251 |
| Remote: | Yes |
| Local: | No |
| Published: | Jan 18 2018 12:00AM |
| Updated: | Jan 18 2018 12:00AM |
| Credit: | Oleg Gaidarenko |
| Vulnerable: | Oracle WebCenter Sites 11.1.1 8.0<br>Oracle Service Bus 12.2.1.3.0<br>Oracle Service Bus 12.1.3.0.0<br>Oracle Primavera Gateway 17.12<br>Oracle Primavera Gateway 16.2<br>Oracle Primavera Gateway 15.2<br>Oracle Hospitality Materials Control 18.1<br>Oracle Hospitality Guest Access 4.2.1<br>Oracle Hospitality Guest Access 4.2<br>Oracle Healthcare Translational Research 3.1 |

SecurityFocus

# VIEM - Dataset

**Joomla! Multiple Flaws Let Remote Authenticated Users Modify ACLs and Execute Arbitrary Code, Remote Users Obtain Potentially Sensitive Information and Conduct Cross-Site Scripting Attacks, and Local Users Obtain Passwords**

**SecurityTracker Alert ID:** 1040966

**SecurityTracker URL:** http://securitytracker.com/id/1040966

**CVE Reference:** CVE-2018-11321, CVE-2018-11322, CVE-2018-11323, CVE-2018-11324, CVE-2018-11325, CVE-2018-11326, CVE-2018-11327, CVE-2018-11328, CVE-2018-6378 *(Links to External Site)*

**Date:** May 23 2018

**Impact:** Disclosure of authentication information, Disclosure of system information, Disclosure of user information, Execution of arbitrary code via network, Modification of system information, Modification of user information, User access via network

**Fix Available:** Yes **Vendor Confirmed:** Yes

**Version(s):** 1.5.0 - 3.8.7

**Description:** Multiple vulnerabilities were reported in Joomla!. A remote authenticated user can modify data on the target system. A remote authenticated user can execute arbitrary code on the target system. A remote user can obtain potentially sensitive information on the target system. A remote user can conduct cross-site scripting attacks. A local user can view the administrator password in certain cases.

SecurityTracker

# VIEM - Dataset

**Vincent Danen** **2011-08-20 00:28:58 EDT** **Description**

A response splitting flaw in Ruby on Rails 2.3.x was reported [1] that could allow a remote attacker to inject arbitrary HTTP headers into a response ... (3.0.0 and later are not vulnerable). Patches are available in the advisory [1] and git [2].

[1] http://groups.google.com/group/rubyonrails-security/browse_thread/thread/6ffc93bde0298768
[2] https://github.com/rails/rails/commit/11dafeaa7533be26441a63618be93a03869c83a9

Openwall

# VIEM - Dataset

3. Problem Description

Horizon 6, 7, and Horizon Client for Windows contain an out-of-bounds read vulnerability in the Message Framework library. Successfully exploiting this issue may allow a less-privileged user to leak information from a privileged process running on a system where Horizon Connection Server, Horizon Agent or Horizon Client are installed.

SecF Forum

# VIEM - Evaluating NER/RE models

| Metric | Precision | Recall | Accuracy |
|---|---|---|---|
| Result | 0.9411 | 0.9932 | 0.9764 |

Over "Memory Corruption" Category

1. G-truth dataset (3,448 CVE IDs) with a ratio 8:1:1 for training, validation, and testing
2. Near 100% accuracy, the state-of-the-art is no higher than 90%

# VIEM - Evaluating Transfer Learning

| Metric | Before Transfer | After Transfer |
|---|---|---|
| Accuracy | 0.8760 | 0.9044 |

Avg. over 12 vulnerability categories

1. Teacher Model - "Memory Corruption" Category (3448 reports), Student Model - other 12 categories (145 reports per cate.)
2. G-truth dataset with a ratio of 1:1 for pre-training, and testing
3. Solved inadequate training dataset issue, and improved accuracy

# In This Paper,

Part I: VIEM - an automatic system

extract vulnerable software name and versions

Part II: Large-scale Measurement

quantify inconsistency and interesting findings

# Metrics

1. Match software names - # of same words > # of different words

"Internet Explorer" and "Microsoft Internet Explorer" ✓

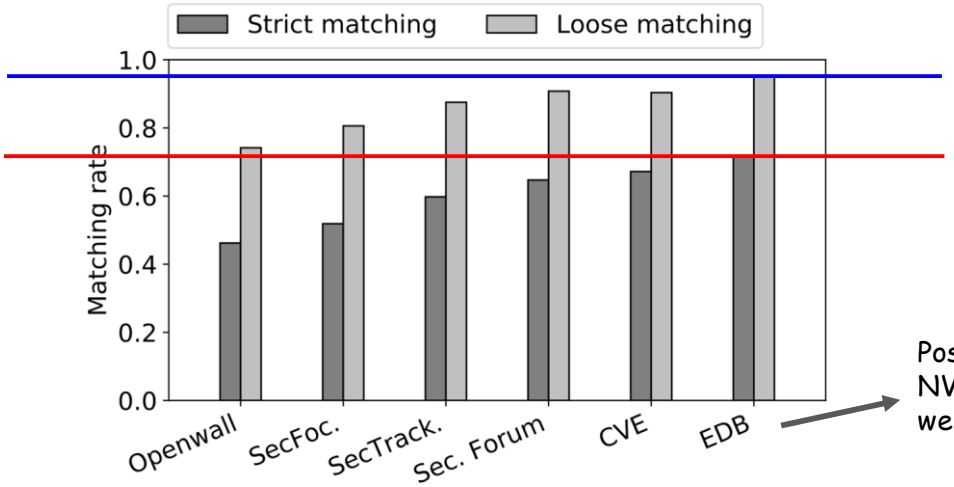
2. Measure version consistency - Strict match vs. Loose match

"1.1" and "from 1.0 to 1.4" ---(CPE directory from NIST)---> [1.1] and [1.0, 1.1, 1.2, 1.3, 1.4]

Strict match (Exact match) ✗

Loose match (One covers another ) ✓

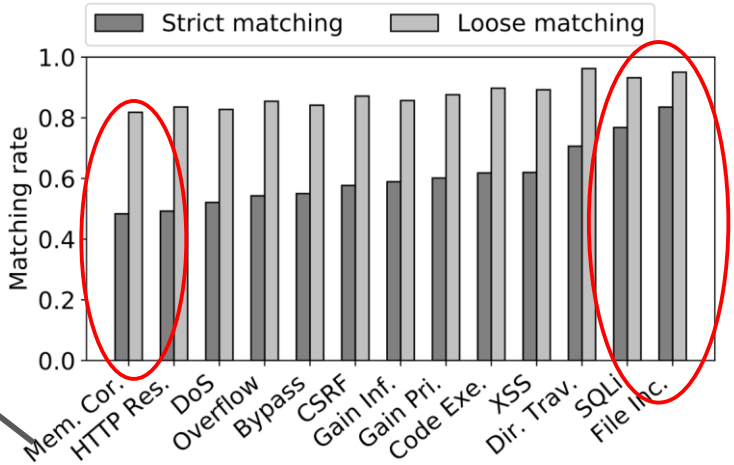
# Inconsistency Exists Among All Vuln. Report Websites




Matching against NVD - official vulnerability report database maintained by U.S. government

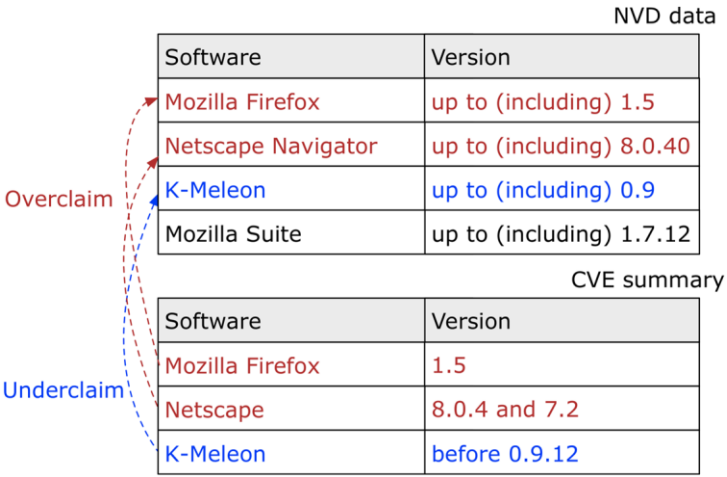
# Inconsistency Exists For All Vuln. Categories

More complex and requires longer time to reproduce and validate.



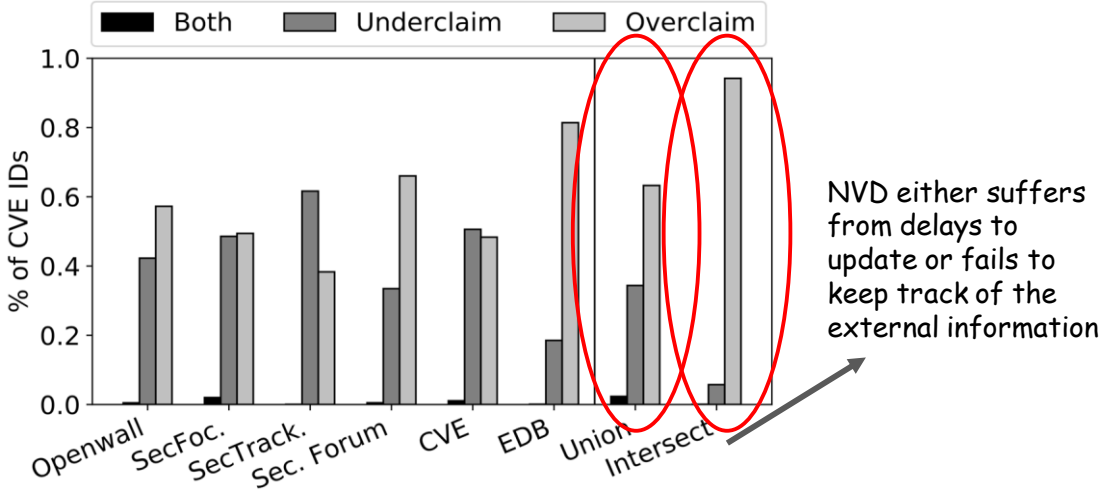

Matching rate for different vulnerability categories - (CVE + 5 websites) vs. NVD

# Inconsistency: Overclaim vs. Underclaim



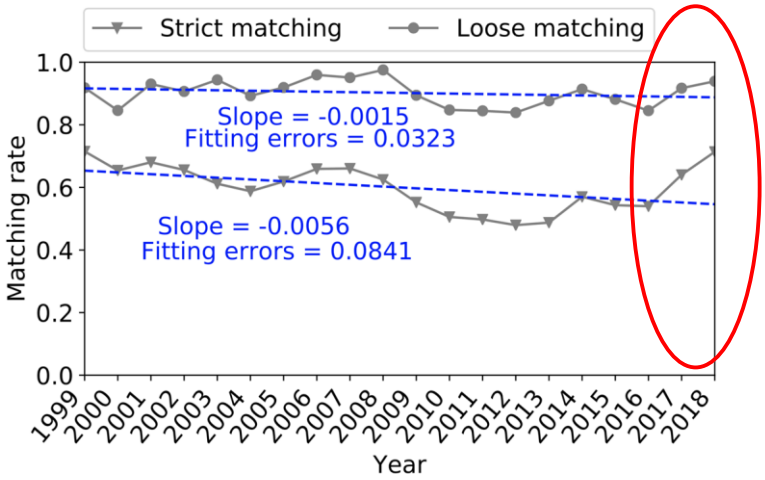

Compared against CVE,
NVD overclaims/underclaims vulnerable versions

# Overclaim/Underclaim Are Both Common




Percentage of Underclaim/Overclaim using loose match: (CVE + 5 websites) vs. NVD

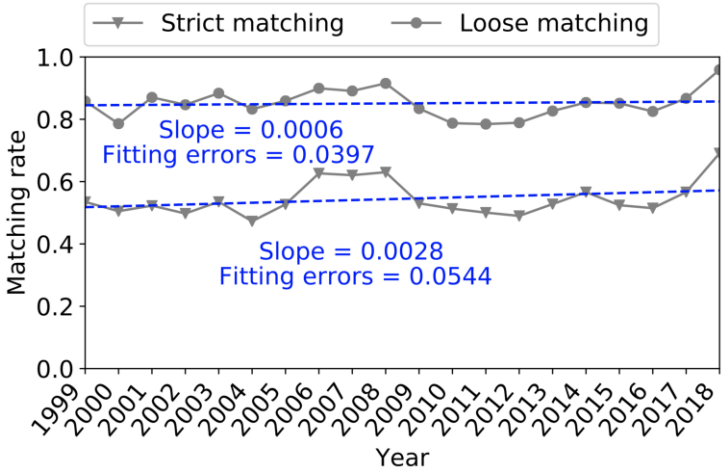
# Inconsistency Rate Varies Over Time




NVD are getting better at summarizing vulnerability versions.

Consistency rate over time: (CVE + 5 websites) vs. NVD

# Inconsistency Rate Varies Over Time




Consistency rate over time: 5 websites vs. CVE

# Reasons of Inconsistency - 1

- Typos

NVD data / CVE summary

| Software | Version |
|---|---|
| Videolan VLC media player | 0.8.6 |

SecurityFocus

| Software | Version |
|---|---|
| Videolan VLC media player | 0.6.8 |

CVE-2010-0364

# Reasons of Inconsistency - 2

- Most reports are seldom updated once created
  ➔ 66.3% of the NVD entries have never been updated


CVE-2006-6516

# Security Implications - Case Study

- 7 real-world vulnerabilities, 47 reports
- 3 security researchers, 185 versions, 4 months' manual verification
- 64 versions are confirmed vulnerable
- 12 newly discovered vulnerable versions

# Security Implication - Case Study (cont.)

| CVE ID | NVD | Intersection Of 5 Sites | Union Of 5 Sites | Ground truth |
|---|---|---|---|---|
| CVE-2004-2167 latex2rtf | 1.9.15 (1) | 1.9.15 (1) | 1.9.15 and possibly others (40) | 1.9.15 (1) |
| CVE-2008-2950 poppler | ≤ 0.8.4 (34) | ≤ 0.8.4 (34) | ≤ 0.8.4 (34) | **0.5.9 - 0.8.4 (16)** |
| CVE-2009-5018 gif2png | 0.99 - 2.5.3 (36) | ≤ 2.5.3 (36) | ≤ 2.5.3 (36) | **2.4.2 - 2.5.6 (13)** |
| CVE-2015-7805 libsndfile | 1.0.25 (1) | 1.0.25 (1) | 1.0.25 (1) | **1.0.15 - 1.0.25 (11)** |
| CVE-2016-7445 openjpeg | ≤ 2.1.1 (16) | 2.1.1 (1) | 2.1.1 (1) | **1.5 - 2.1.1 (7)** |
| CVE-2016-8676 libav | ≤ 11.8 (47) | 11.3, 11.4, 11.5, 11.7 (4) | 11.3, 11.4, 11.5, 11.7, 11.8, 11.9 (4) | **11.0 - 11.8 (9)** |
| CVE-2016-9556 ImageMagick | 7.0.3.8 (1) | 7.0.3.6 | 7.0.3.6, 7.0.3.8 (2) | **7.0.3.1 - 7.0.3.7 (7)** |

# Conclusion

1. VIEM - an automatic tool to detect inconsistency in Vuln. reports
2. A large - scale measurement of the information consistency
3. Case study - validated inconsistent information (and show its impact)

# Open Challenges

1. Standardize vulnerability reporting procedure
2. Design a fully automated system to verify the vulnerability reported

# Thank you

Code & Data

https://github.com/pinkymm/inconsistency_detection

Presenter: 欧国亮

https://ougl.cn/