The Life of a BUG REPORT

by Brian Schweigler

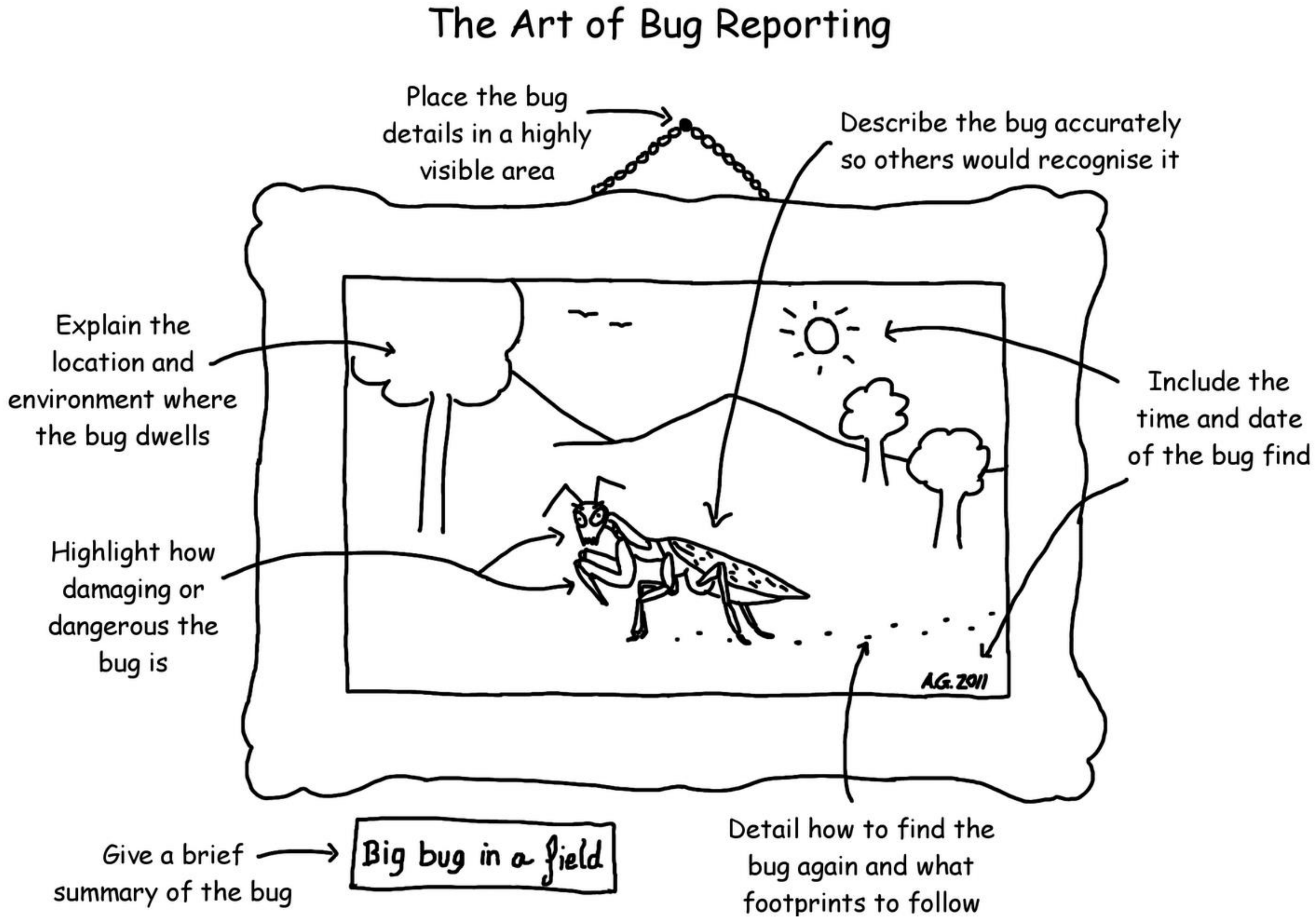
Bachelor Thesis, 1st presentation

15th October 2019

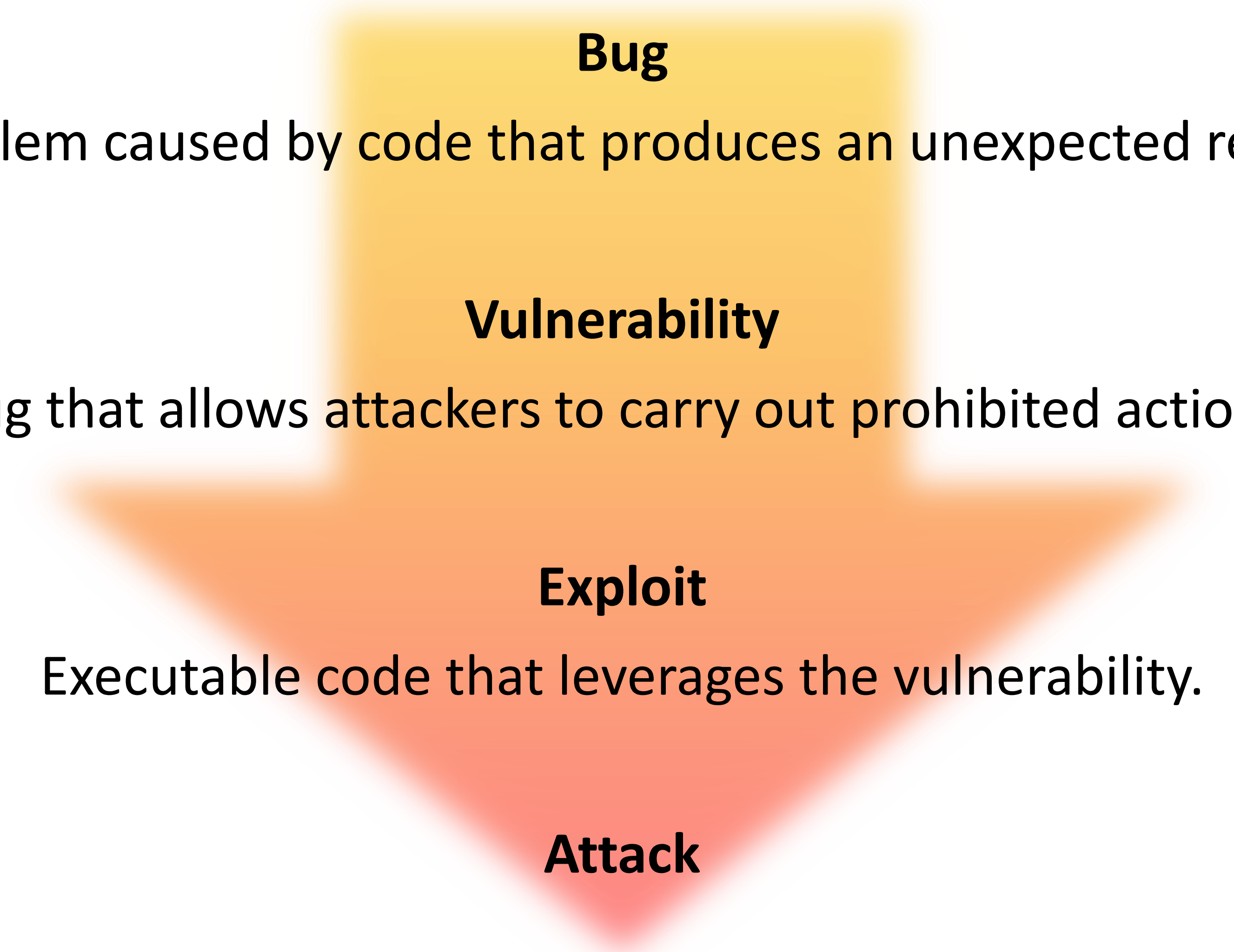
Motivation

> «One does not know all the expected effects of known bugs.»
>
> — Frederick Brooks, The Mythical Man-Month

What is a good bug report?


The Art of Bug Reporting
Place the bug details in a highly visible area
Describe the bug accurately so others would recognise it
Explain the location and environment where the bug dwells
Include the time and date of the bug find
Highlight how damaging or dangerous the bug is
A.G. 2011
Give a brief summary of the bug
Big bug in a field
Detail how to find the bug again and what footprints to follow

From a bug to the attack



Bug

Problem caused by code that produces an unexpected result.

Vulnerability

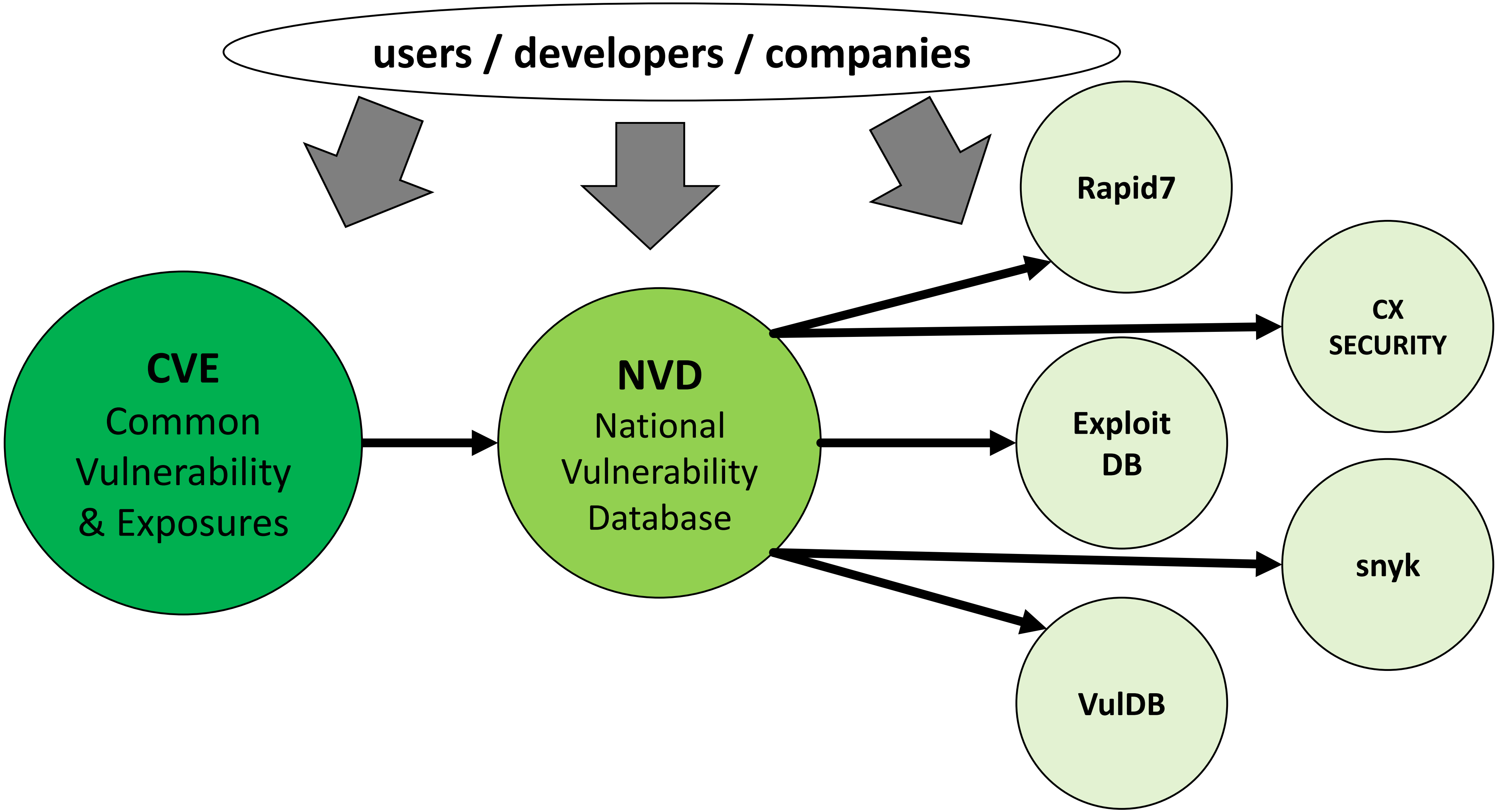
Bug that allows attackers to carry out prohibited actions.

Exploit

Executable code that leverages the vulnerability.

Attack

Propagation of vulnerability reports



users / developers / companies

CVE
Common
Vulnerability
& Exposures

NVD
National
Vulnerability
Database

Rapid7

CX SECURITY

Exploit DB

snyk

VulDB

Preliminary research questions

RQ1:

What are the commonly used criteria in bug reports, and how are they used?

RQ2:

How and when are reports propagated between the various databases?
Can we find any trends?

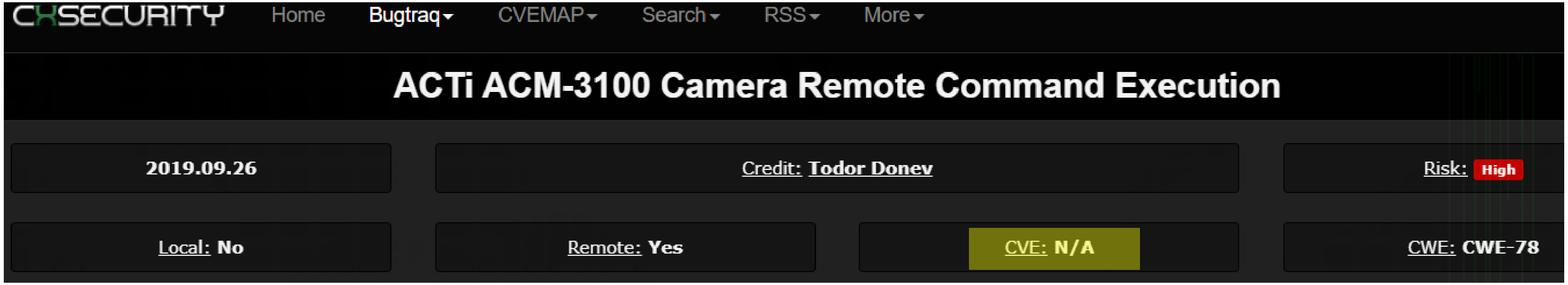
RQ3:

What is the role and reliability of the used vulnerability score metrics?

RQ1
(Criteria)

Notable observation #1

Missing data



ACTi ACM-3100 Camera Remote Command Execution

2019.09.26

Credit: Todor Donev

Risk: High

Local: No

Remote: Yes

CVE: N/A

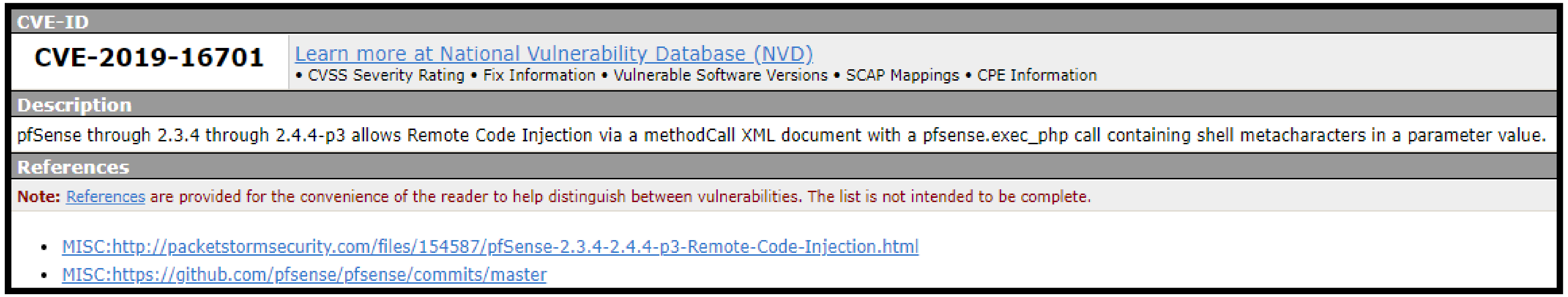
CWE: CWE-78

significance?

RQ1
(Criteria)

Notable observation #2

Harmful data



CVE-ID

CVE-2019-16701

Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

pfSense through 2.3.4 through 2.4.4-p3 allows Remote Code Injection via a methodCall XML document with a pfsense.exec_php call containing shell metacharacters in a parameter value.

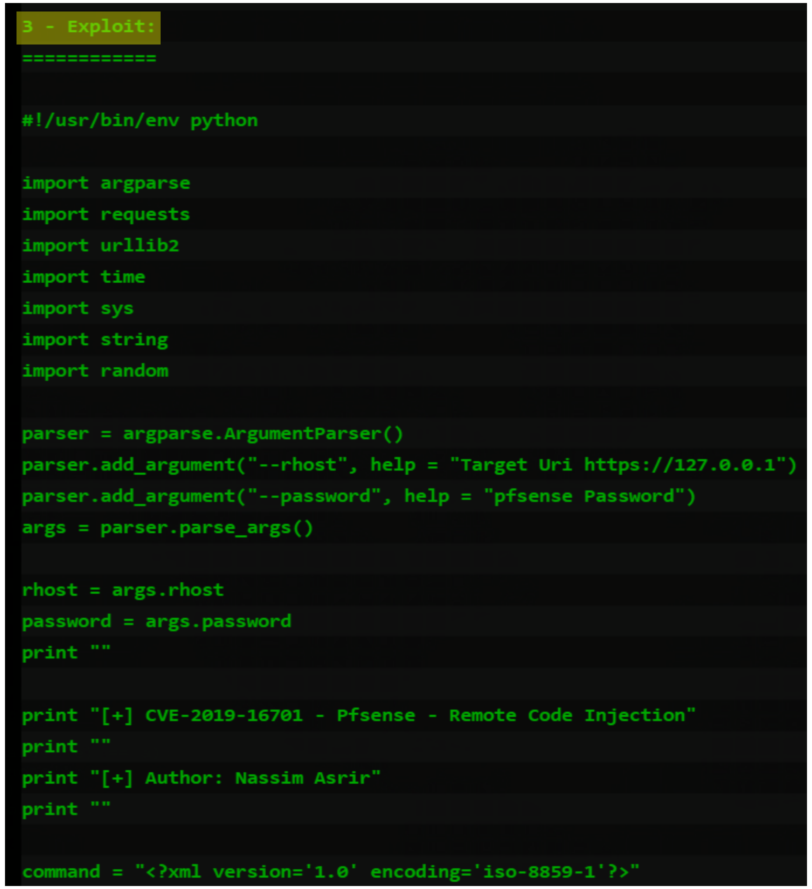
References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:http://packetstormsecurity.com/files/154587/pfSense-2.3.4-2.4.4-p3-Remote-Code-Injection.html
- MISC:https://github.com/pfsense/pfsense/commits/master

Availability of

Proof-of-Concept?
Exploit?

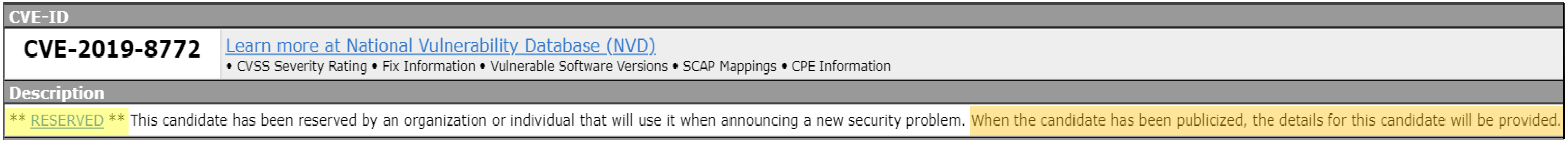


```
3 - Exploit:
============

#!/usr/bin/env python

import argparse
import requests
import urllib2
import time
import sys
import string
import random

parser = argparse.ArgumentParser()
parser.add_argument("--rhost", help = "Target Uri https://127.0.0.1")
parser.add_argument("--password", help = "pfsense Password")
args = parser.parse_args()

rhost = args.rhost
password = args.password
print ""

print "[+] CVE-2019-16701 - Pfsense - Remote Code Injection"
print ""
print "[+] Author: Nassim Asrir"
print ""

command = "<?xml version='1.0' encoding='iso-8859-1'?>"
```

RQ2
(Propagation)

Notable observation #3

Information leak before «official» disclosure



CVE-ID

CVE-2019-8772

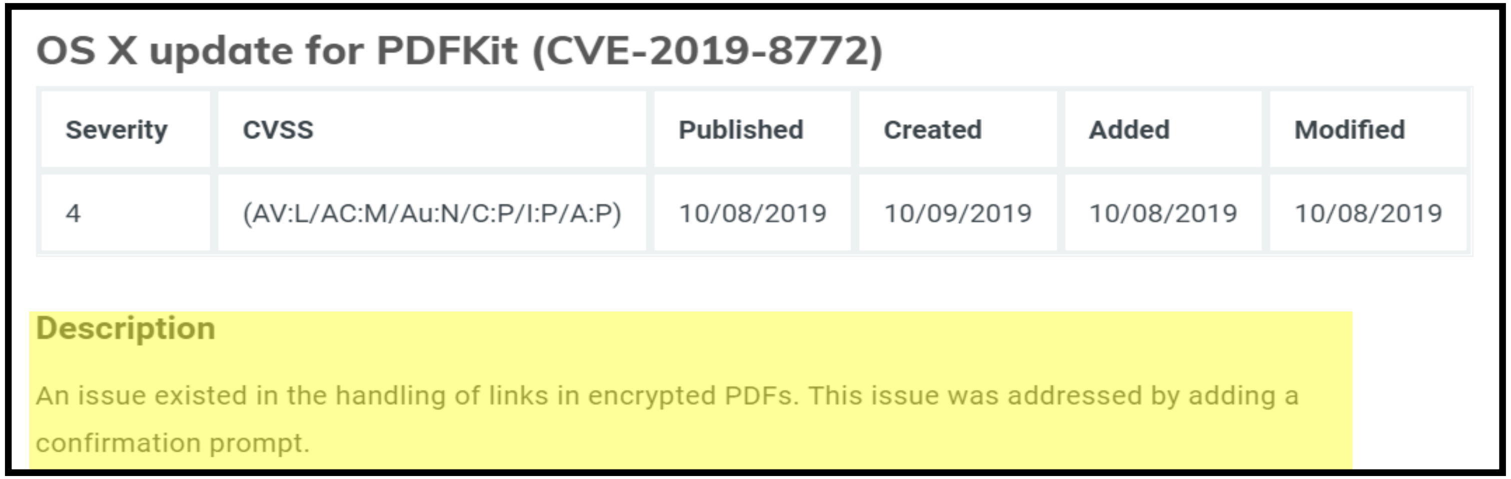
Learn more at National Vulnerability Database (NVD)

• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

?



OS X update for PDFKit (CVE-2019-8772)

Severity	CVSS	Published	Created	Added	Modified
4	(AV:L/AC:M/Au:N/C:P/I:P/A:P)	10/08/2019	10/09/2019	10/08/2019	10/08/2019

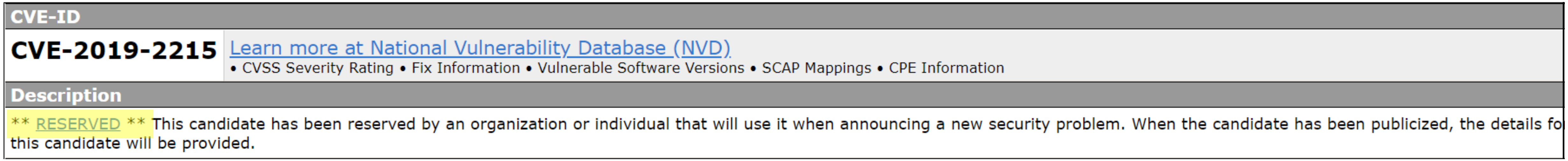
Description

An issue existed in the handling of links in encrypted PDFs. This issue was addressed by adding a confirmation prompt.

RQ2
(Propagation)

Notable observation #4

Information leak before «official» disclosure



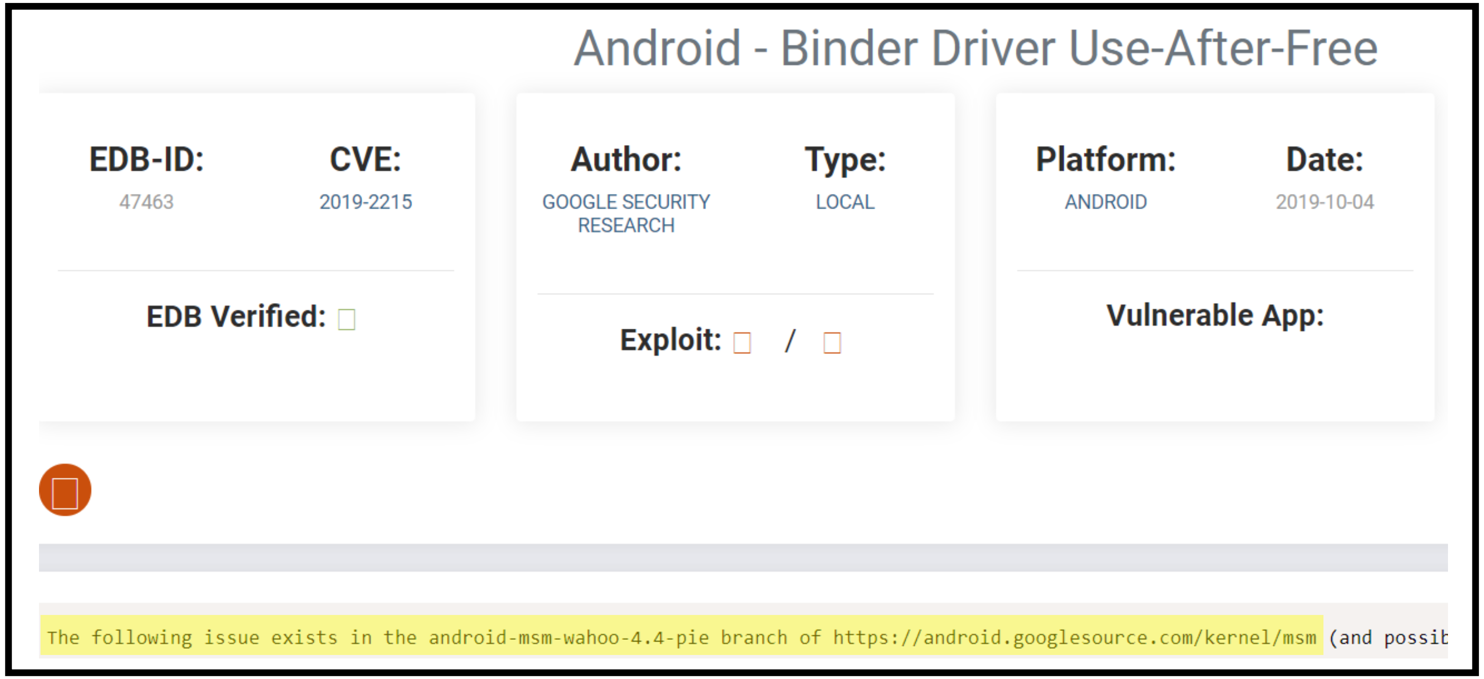
CVE-ID

CVE-2019-2215 [Learn more at National Vulnerability Database (NVD)]
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details fo
this candidate will be provided.

?



Android - Binder Driver Use-After-Free

EDB-ID:	**CVE:**	**Author:**	**Type:**	**Platform:**	**Date:**
47463	2019-2215	GOOGLE SECURITY RESEARCH	LOCAL	ANDROID	2019-10-04

EDB Verified: □

Exploit: □ / □

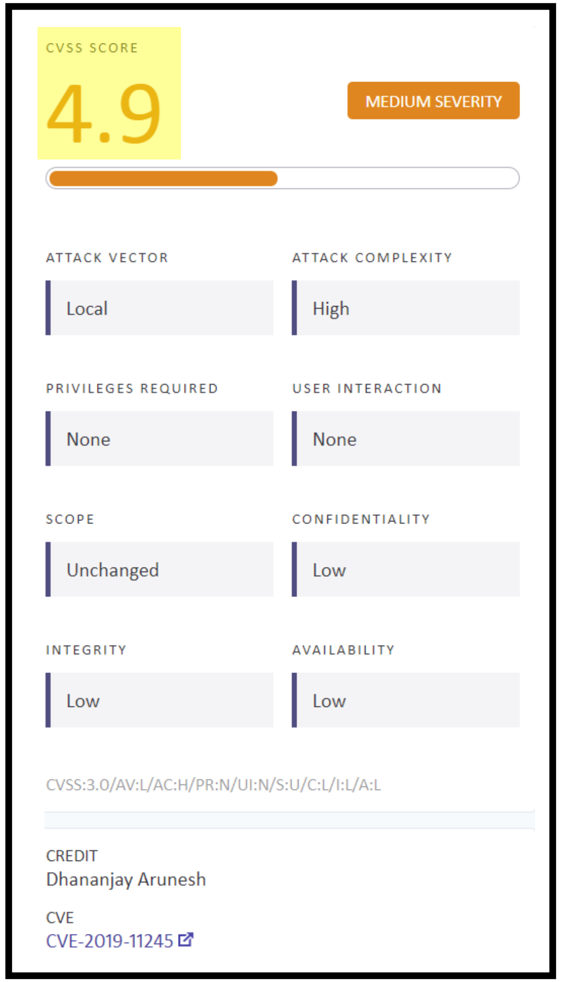
Vulnerable App:

```
The following issue exists in the android-msm-wahoo-4.4-pie branch of https://android.googlesource.com/kernel/msm (and possit
```

RQ3 (Metrics)

Notable observation #5

Scores diverge



CVSS SCORE

4.9

MEDIUM SEVERITY

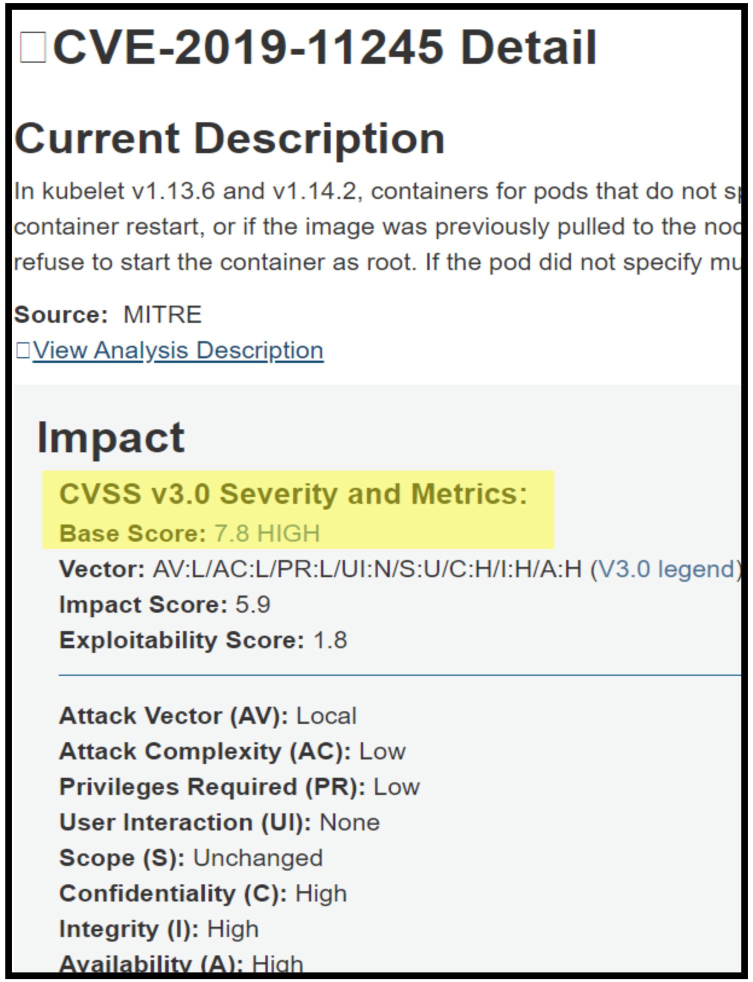
ATTACK VECTOR	ATTACK COMPLEXITY
Local	High
PRIVILEGES REQUIRED	**USER INTERACTION**
None	None
SCOPE	**CONFIDENTIALITY**
Unchanged	Low
INTEGRITY	**AVAILABILITY**
Low	Low

CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L

CREDIT
Dhananjay Arunesh

CVE
CVE-2019-11245

?



CVE-2019-11245 Detail

Current Description

In kubelet v1.13.6 and v1.14.2, containers for pods that do not s
container restart, or if the image was previously pulled to the noc
refuse to start the container as root. If the pod did not specify mu

Source: MITRE

View Analysis Description

Impact

CVSS v3.0 Severity and Metrics:

Base Score: 7.8 HIGH

Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H (V3.0 legend)

Impact Score: 5.9

Exploitability Score: 1.8

Attack Vector (AV): Local

Attack Complexity (AC): Low

Privileges Required (PR): Low

User Interaction (UI): None

Scope (S): Unchanged

Confidentiality (C): High

Integrity (I): High

Availability (A): High

Next Steps

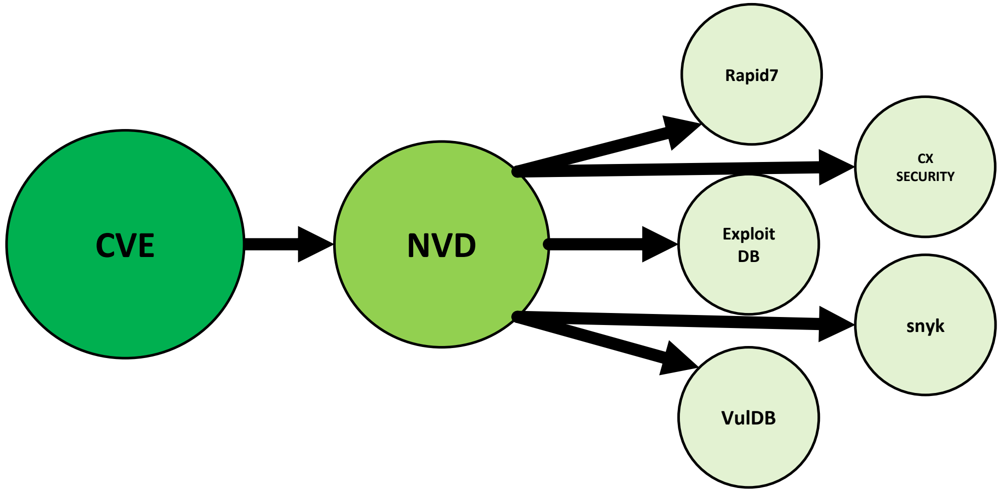
1. **Download or parse** data from vulnerability database websites

2. **Reverse bug report look ups** to collect initial reports from accessible repositories

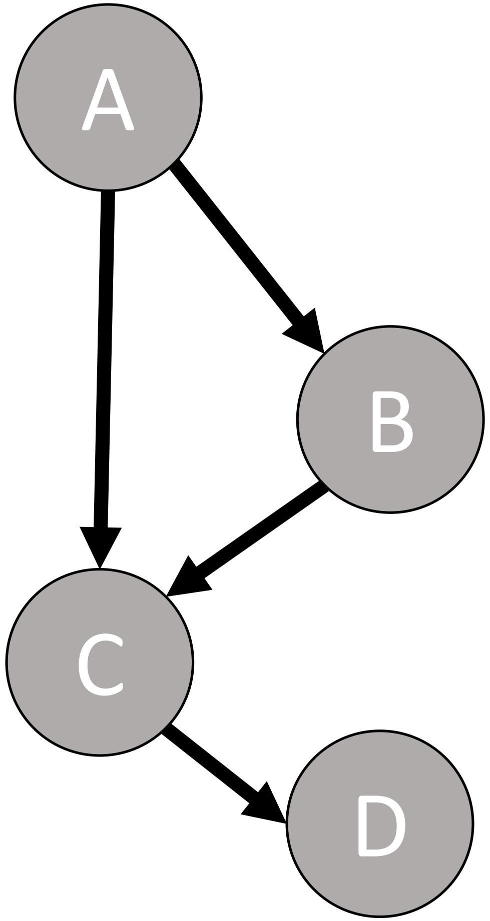
3. **Search** within the data for outliers and trends

4. **Distill findings for advice** towards developers, security researchers & end users

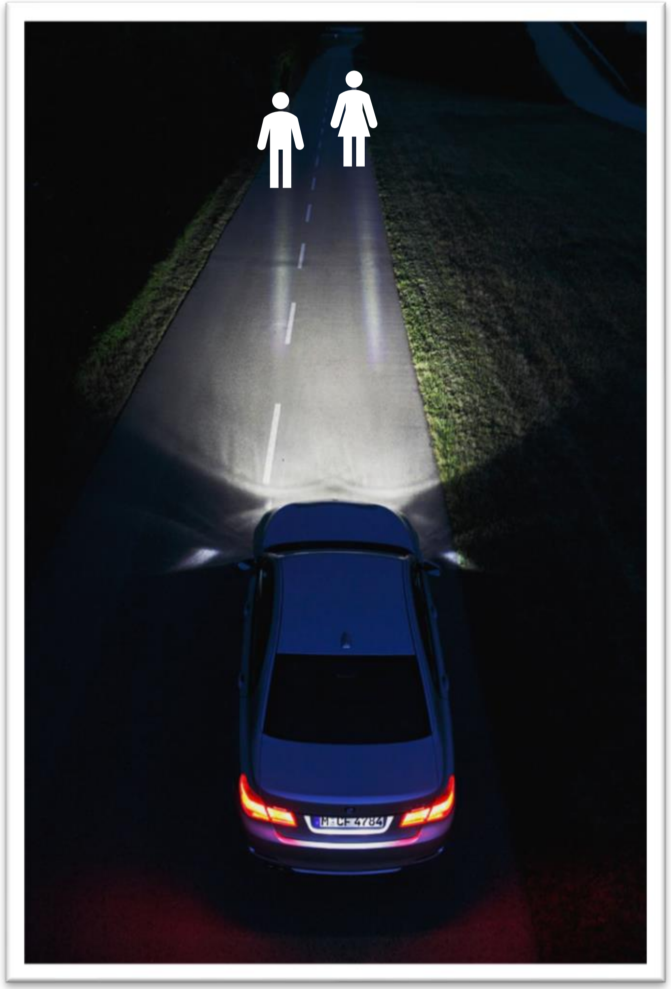
Summary



Unstructured & distributed information



Solution



Vision

Sources

- “Ladybird Clipart”, Meladee
  https://www.cleanpng.com/png-rhinoceros-beetles-polyphaga-japanese-rhinoceros-b-7024001/
- “The Art of Bugreporting”, Andy Glover
  http://cartoontester.blogspot.com/
- Sources for definitions and background information (Slide 4)

  https://www.kb.cert.org/vuls/guidance/ *09.10.19 (18:00)*

  https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/ *09.10.19 (18:00)*

  https://www.gizmosphere.org/network-security-vulnerabilities-vs-exploits/ *09.10.19 (18:00)*