VerDiff : Vulnerability Presence Verification for Comprehensive Reporting Using Constraint Programming

Md Sakib Anwar
anwar.40@osu.edu

Carter Yagemann
yagemann.1@osu.edu

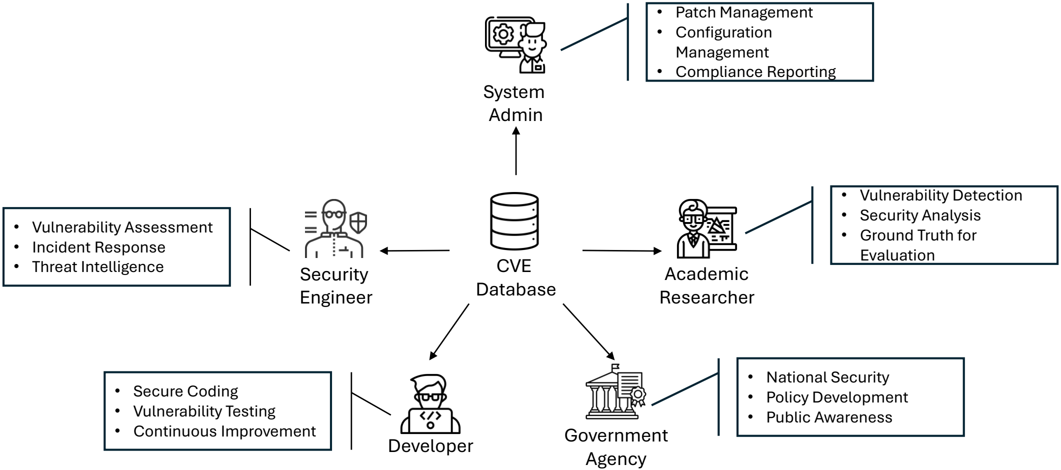
Zhiqiang Lin
zlin@cse.ohio-state.edu

December 10, ACSAC 2025

The Ohio State University

Introduction

CVEs as Central Source of Information



System Admin

- Patch Management
- Configuration Management
- Compliance Reporting

CVE Database

Security Engineer

- Vulnerability Assessment
- Incident Response
- Threat Intelligence

Academic Researcher

- Vulnerability Detection
- Security Analysis
- Ground Truth for Evaluation

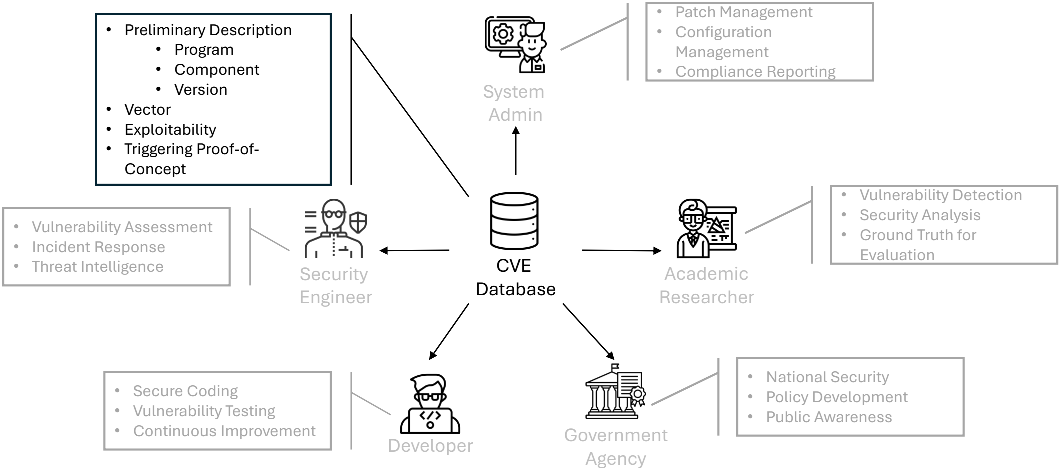
Developer

- Secure Coding
- Vulnerability Testing
- Continuous Improvement

Government Agency

- National Security
- Policy Development
- Public Awareness

CVEs as Central Source of Information



- Preliminary Description
  - Program
  - Component
  - Version
- Vector
- Exploitability
- Triggering Proof-of-Concept

CVE Database

System Admin

- Patch Management
- Configuration Management
- Compliance Reporting

Security Engineer

- Vulnerability Assessment
- Incident Response
- Threat Intelligence

Academic Researcher

- Vulnerability Detection
- Security Analysis
- Ground Truth for Evaluation

Developer

- Secure Coding
- Vulnerability Testing
- Continuous Improvement

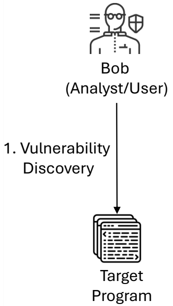
Government Agency

- National Security
- Policy Development
- Public Awareness

Vulnerability Discovery & Reporting

Bob
(Analyst/User)

Vulnerability Discovery & Reporting

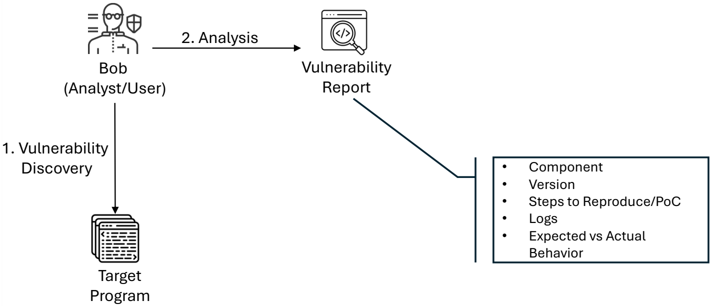


Bob (Analyst/User)

1. Vulnerability Discovery

Target Program

Vulnerability Discovery & Reporting



Bob (Analyst/User)

1. Vulnerability Discovery

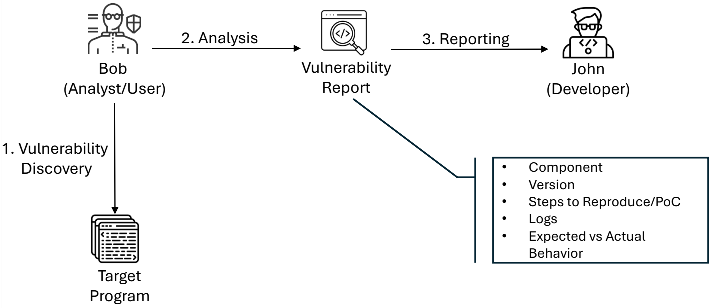
Target Program

2. Analysis

Vulnerability Report

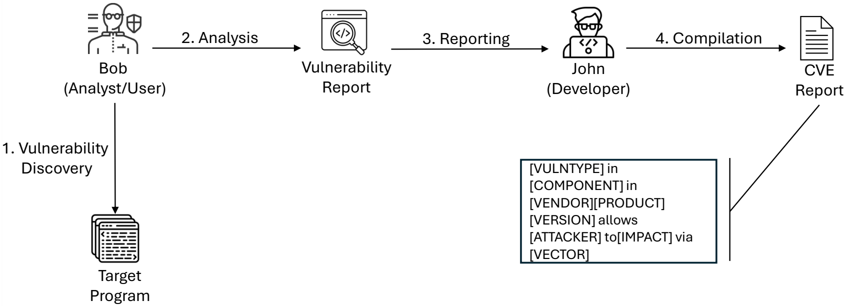
- Component
- Version
- Steps to Reproduce/PoC
- Logs
- Expected vs Actual Behavior

Vulnerability Discovery & Reporting



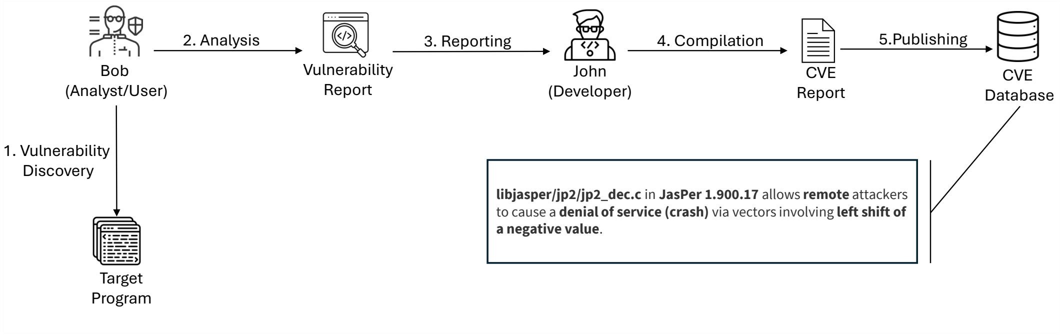
- Component
- Version
- Steps to Reproduce/PoC
- Logs
- Expected vs Actual Behavior

Vulnerability Discovery & Reporting



[VULNTYPE] in [COMPONENT] in [VENDOR][PRODUCT] [VERSION] allows [ATTACKER] to[IMPACT] via [VECTOR]

Vulnerability Discovery & Reporting



Bob (Analyst/User)

2. Analysis

Vulnerability Report

3. Reporting

John (Developer)

4. Compilation

CVE Report

5.Publishing

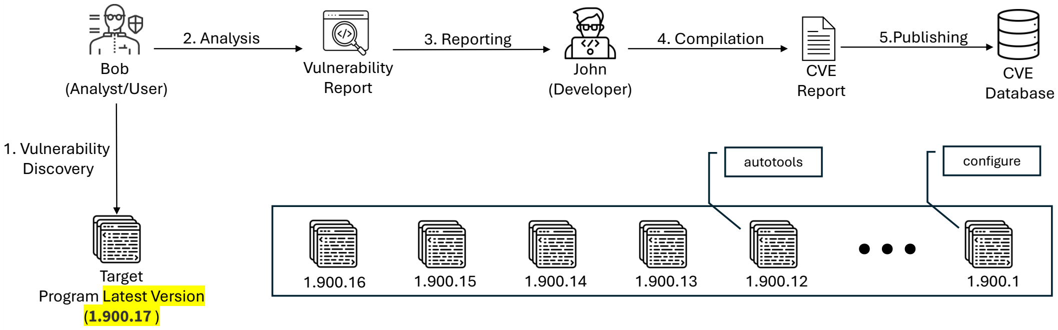
CVE Database

1. Vulnerability Discovery

Target Program

libjasper/jp2/jp2_dec.c in **JasPer 1.900.17** allows **remote** attackers to cause a **denial of service (crash)** via vectors involving **left shift of a negative value**.

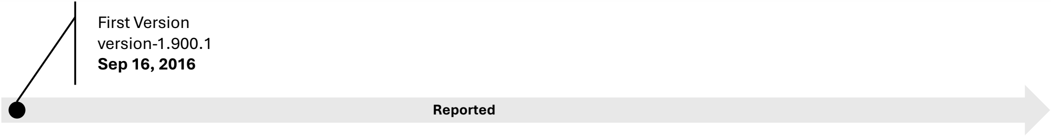
Problems in Current Reporting System



- **81.5%** systems contains outdated dependencies
- Syzbot identifies compiling **outdated versions** as one of the key reasons of inability to analyze a program

Background

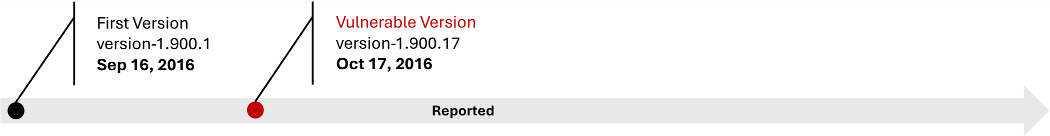
Motivating Example: CVE-2017-5502 of Jasper



First Version
version-1.900.1
Sep 16, 2016

Reported

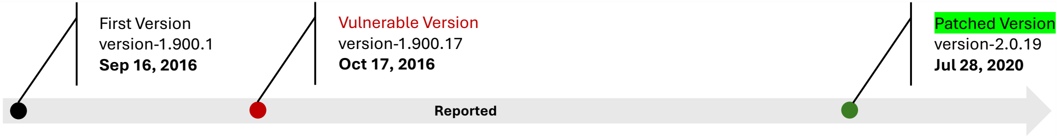
Motivating Example: CVE-2017-5502 of Jasper



First Version
version-1.900.1
Sep 16, 2016

Vulnerable Version
version-1.900.17
Oct 17, 2016

Motivating Example: CVE-2017-5502 of Jasper



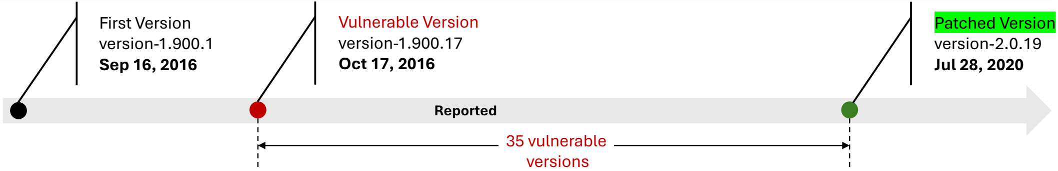
First Version
version-1.900.1
Sep 16, 2016

Vulnerable Version
version-1.900.17
Oct 17, 2016

Patched Version
version-2.0.19
Jul 28, 2020

Reported

Motivating Example: CVE-2017-5502 of Jasper



First Version
version-1.900.1
Sep 16, 2016

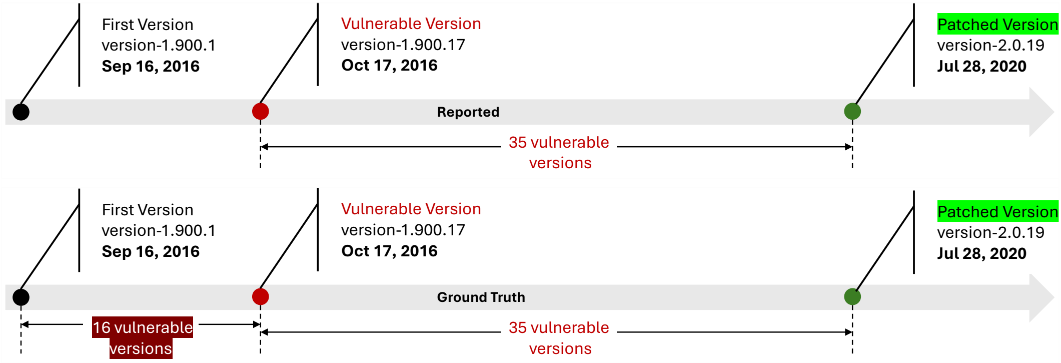
Vulnerable Version
version-1.900.17
Oct 17, 2016

Patched Version
version-2.0.19
Jul 28, 2020

Reported

35 vulnerable versions

Motivating Example: CVE-2017-5502 of Jasper



First Version
version-1.900.1
Sep 16, 2016

Vulnerable Version
version-1.900.17
Oct 17, 2016

Patched Version
version-2.0.19
Jul 28, 2020

Reported

35 vulnerable versions

First Version
version-1.900.1
Sep 16, 2016

Vulnerable Version
version-1.900.17
Oct 17, 2016

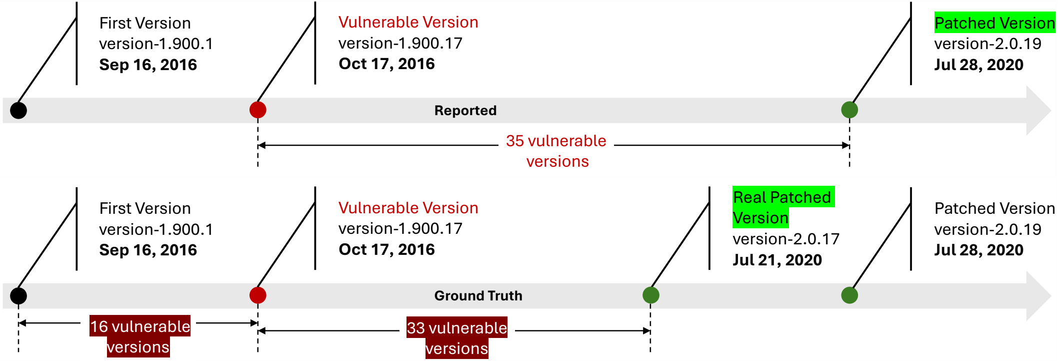
Patched Version
version-2.0.19
Jul 28, 2020

Ground Truth

16 vulnerable versions

35 vulnerable versions

Motivating Example: CVE-2017-5502 of Jasper



Design

Steps for Known Vulnerability Detection

1. Vulnerable Code Identification
2. Signature Creation
3. Signature Matching

```
int jp2_validate(jas_stream_t *in)
{
  char buf[JP2_VALIDATELEN];
...
  if ((n = jas_stream_read(in, buf,
          JP2_VALIDATELEN)) < 0) {
    return -1;
  }
...
  for (i = n - 1; i >= 0; --i) {
    if (jas_stream_ungetc(in, buf[i]) == EOF) {
      return -1;
    }
  }
...
  if (((buf[4] << 24) | (buf[5] << 16) |
          (buf[6] << 8) | buf[7]) !=
                 JP2_BOX_JP)
  {
    return -1;
  }
...
}
```

Vulnerable Code in Jasper 1.900.17:jp2_dec.c

Step 1: Vulnerable Code Identification

```
int jp2_validate(jas_stream_t *in)
{
 char buf[JP2_VALIDATELEN];
...
 if ((n = jas_stream_read(in, buf,
     JP2_VALIDATELEN)) < 0) {
  return -1;
 }
...
 for (i = n - 1; i >= 0; --i) {
  if (jas_stream_ungetc(in, buf[i]) == EOF) {
   return -1;
  }
 }
...
 if (((buf[4] << 24) | (buf[5] << 16) |
     (buf[6] << 8) | buf[7]) !=
          JP2_BOX_JP)
 {
  return -1;
 }
...
}
```

Vulnerable Code in Jasper 1.900.17:jp2_dec.c

Step 1: Vulnerable Code Identification

Existing Approach

1. Prexisting signature can detect vulnerability with high confidence

Cons of Approach

1. Requires manual update for novel vulnerability

```
453 int jp2_validate(jas_stream_t *in)
454 {
455   char buf[JP2_VALIDATELEN];
...
467   if ((n = jas_stream_read(in, buf,
              JP2_VALIDATELEN)) < 0) {
468     return -1;
469   }
...
473   for (i = n - 1; i >= 0; --i) {
474     if (jas_stream_ungetc(in, buf[i]) == EOF) {
475       return -1;
476     }
477   }
...
485   if (((buf[4] << 24) | (buf[5] << 16) |
             (buf[6] << 8) | buf[7]) !=
486                  JP2_BOX_JP)
487   {
488     return -1;
489   }
...
492 }
```

Vulnerable Code in Jasper 1.900.17:jp2_dec.c

Step 1: Vulnerable Code Identification

Existing Approach

1. Prexisting signature can detect vulnerability with high confidence
2. Patch can locate the vulnerability

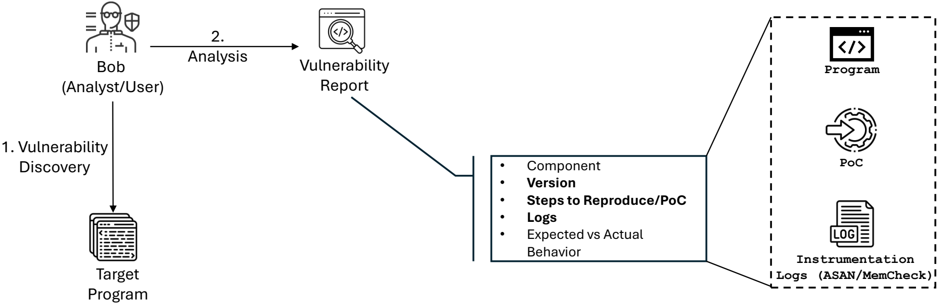
Cons of Approach

1. Requires manual update for novel vulnerability
2. Patch release can take on average **256 days**

```
int jp2_validate(jas_stream_t *in)
{
  char buf[JP2_VALIDATELEN];
...
  if ((n = jas_stream_read(in, buf,
          JP2_VALIDATELEN)) < 0) {
    return -1;
  }
...
  for (i = n - 1; i >= 0; --i) {
    if (jas_stream_ungetc(in, buf[i]) == EOF) {
      return -1;
    }
  }
...
  if (((buf[4] << 24) | (buf[5] << 16) |
          (buf[6] << 8) | buf[7]) !=
                    JP2_BOX_JP)
  {
    return -1;
  }
...
}
```

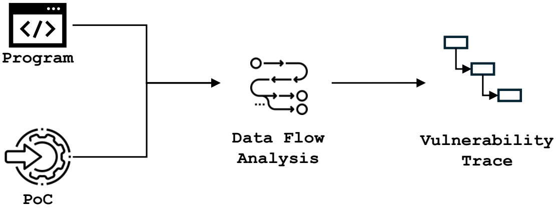
Vulnerable Code in Jasper 1.900.17:jp2_dec.c

Step 1: Vulnerable Code Identification

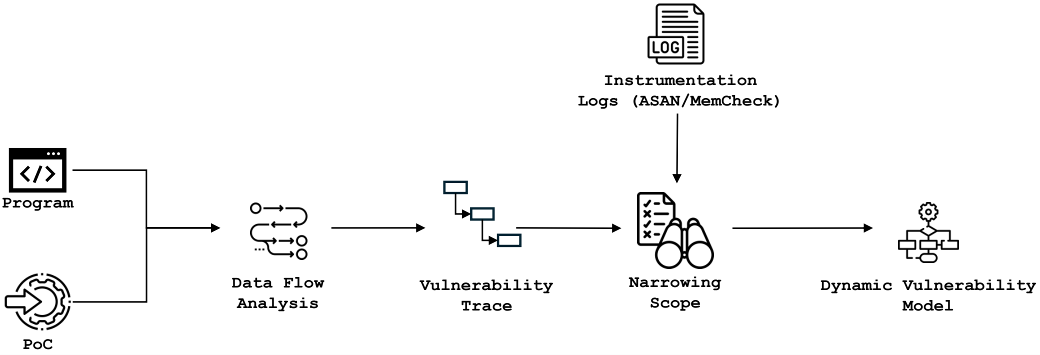


- Component
- **Version**
- **Steps to Reproduce/PoC**
- **Logs**
- Expected vs Actual Behavior

Step 1: Vulnerable Code Identification



Step 1: Vulnerable Code Identification



Step 2: Signature Creation

- Is source code matching enough?

```
int jp2_validate(jas_stream_t *in)
{
  char buf[JP2_VALIDATELEN];
...
  if ((n = jas_stream_read(in, buf,
          JP2_VALIDATELEN)) < 0) {
    return -1;
  }
...
  for (i = n - 1; i >= 0; --i) {
    if (jas_stream_ungetc(in, buf[i]) == EOF) {
      return -1;
    }
  }
...
  if (((buf[4] << 24) | (buf[5] << 16) |
          (buf[6] << 8) | buf[7]) !=
                    JP2_BOX_JP)
  {
    return -1;
  }
...
}
```

Step 2: Signature Creation

- Is source code matching enough?
  - Data type
  - Global constants

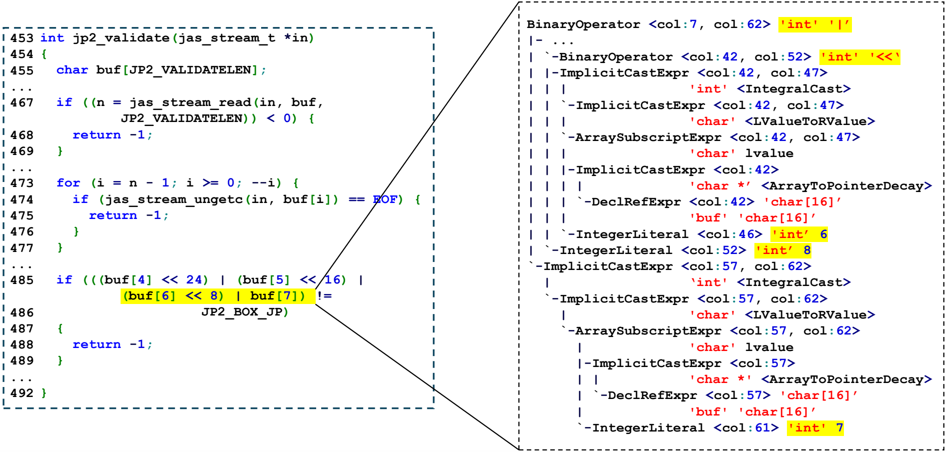
```
int jp2_validate(jas_stream_t *in)
{
  char buf[JP2_VALIDATELEN];
...
  if ((n = jas_stream_read(in, buf,
          JP2_VALIDATELEN)) < 0) {
    return -1;
  }
...
  for (i = n - 1; i >= 0; --i) {
    if (jas_stream_ungetc(in, buf[i]) == EOF) {
      return -1;
    }
  }
...
  if (((buf[4] << 24) | (buf[5] << 16) |
          (buf[6] << 8) | buf[7]) !=
                JP2_BOX_JP)
  {
    return -1;
  }
...
}
```

Step 2: Signature Creation

- Is source code matching enough?
  - Data type
  - Global constants
  - Function side effects

```
int jp2_validate(jas_stream_t *in)
{
  char buf[JP2_VALIDATELEN];
...
  if ((n = jas_stream_read(in, buf,
          JP2_VALIDATELEN)) < 0) {
    return -1;
  }
...
  for (i = n - 1; i >= 0; --i) {
    if (jas_stream_ungetc(in, buf[i]) == EOF) {
      return -1;
    }
  }
...
  if (((buf[4] << 24) | (buf[5] << 16) |
          (buf[6] << 8) | buf[7]) !=
                    JP2_BOX_JP)
  {
    return -1;
  }
...
}
```

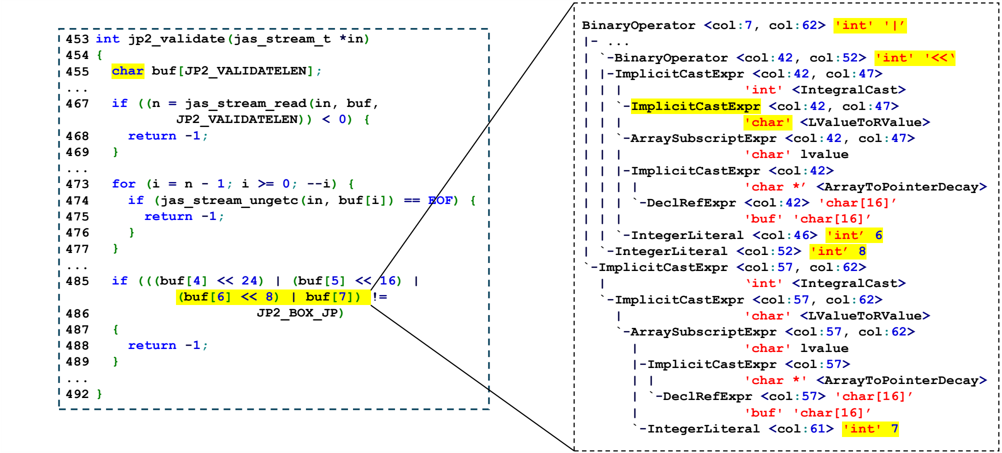
Step 2: Signature Creation



```
int jp2_validate(jas_stream_t *in)
{
  char buf[JP2_VALIDATELEN];
...
  if ((n = jas_stream_read(in, buf,
          JP2_VALIDATELEN)) < 0) {
    return -1;
  }
...
  for (i = n - 1; i >= 0; --i) {
    if (jas_stream_ungetc(in, buf[i]) == EOF) {
      return -1;
    }
  }
...
  if (((buf[4] << 24) | (buf[5] << 16) |
          (buf[6] << 8) | buf[7]) !=
                JP2_BOX_JP)
  {
    return -1;
  }
...
}
```

```
BinaryOperator <col:7, col:62> 'int' '|'
|- ...
| `-BinaryOperator <col:42, col:52> 'int' '<<'
| |-ImplicitCastExpr <col:42, col:47>
| | |            'int' <IntegralCast>
| | `-ImplicitCastExpr <col:42, col:47>
| | |            'char' <LValueToRValue>
| | `-ArraySubscriptExpr <col:42, col:47>
| | |            'char' lvalue
| | |-ImplicitCastExpr <col:42>
| | | |          'char *' <ArrayToPointerDecay>
| | | `-DeclRefExpr <col:42> 'char[16]'
| | |            'buf' 'char[16]'
| | `-IntegerLiteral <col:46> 'int' 6
| `-IntegerLiteral <col:52> 'int' 8
`-ImplicitCastExpr <col:57, col:62>
  |              'int' <IntegralCast>
  `-ImplicitCastExpr <col:57, col:62>
    |            'char' <LValueToRValue>
    `-ArraySubscriptExpr <col:57, col:62>
      |          'char' lvalue
      |-ImplicitCastExpr <col:57>
      | |        'char *' <ArrayToPointerDecay>
      | `-DeclRefExpr <col:57> 'char[16]'
      |          'buf' 'char[16]'
      `-IntegerLiteral <col:61> 'int' 7
```

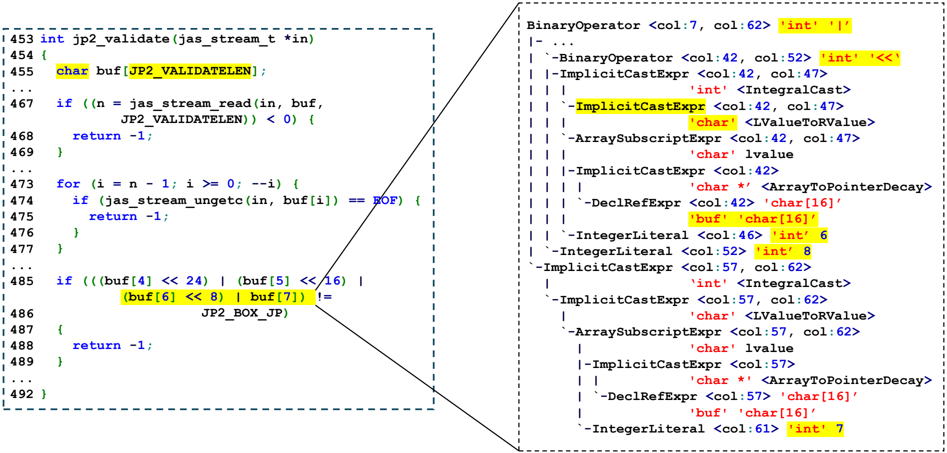
Step 2: Signature Creation



```
int jp2_validate(jas_stream_t *in)
{
  char buf[JP2_VALIDATELEN];
...
  if ((n = jas_stream_read(in, buf,
          JP2_VALIDATELEN)) < 0) {
    return -1;
  }
...
  for (i = n - 1; i >= 0; --i) {
    if (jas_stream_ungetc(in, buf[i]) == EOF) {
      return -1;
    }
  }
...
  if (((buf[4] << 24) | (buf[5] << 16) |
          (buf[6] << 8) | buf[7]) !=
                    JP2_BOX_JP)
  {
    return -1;
  }
...
}
```

```
BinaryOperator <col:7, col:62> 'int' '|'
|- ...
| `-BinaryOperator <col:42, col:52> 'int' '<<'
| |-ImplicitCastExpr <col:42, col:47>
| | |               'int' <IntegralCast>
| | `-ImplicitCastExpr <col:42, col:47>
| | |               'char' <LValueToRValue>
| | `-ArraySubscriptExpr <col:42, col:47>
| | |               'char' lvalue
| | |-ImplicitCastExpr <col:42>
| | | |             'char *' <ArrayToPointerDecay>
| | | `-DeclRefExpr <col:42> 'char[16]'
| | |               'buf' 'char[16]'
| | `-IntegerLiteral <col:46> 'int' 6
| `-IntegerLiteral <col:52> 'int' 8
`-ImplicitCastExpr <col:57, col:62>
  |               'int' <IntegralCast>
  `-ImplicitCastExpr <col:57, col:62>
    |             'char' <LValueToRValue>
    `-ArraySubscriptExpr <col:57, col:62>
      |           'char' lvalue
      |-ImplicitCastExpr <col:57>
      | |         'char *' <ArrayToPointerDecay>
      | `-DeclRefExpr <col:57> 'char[16]'
      |           'buf' 'char[16]'
      `-IntegerLiteral <col:61> 'int' 7
```

Step 2: Signature Creation

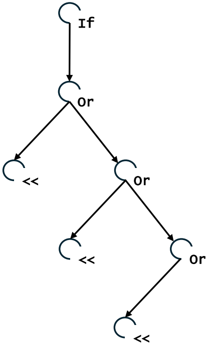


```
453 int jp2_validate(jas_stream_t *in)
454 {
455   char buf[JP2_VALIDATELEN];
...
467   if ((n = jas_stream_read(in, buf,
              JP2_VALIDATELEN)) < 0) {
468     return -1;
469   }
...
473   for (i = n - 1; i >= 0; --i) {
474     if (jas_stream_ungetc(in, buf[i]) == EOF) {
475       return -1;
476     }
477   }
...
485   if (((buf[4] << 24) | (buf[5] << 16) |
              (buf[6] << 8) | buf[7]) !=
486                     JP2_BOX_JP)
487   {
488     return -1;
489   }
...
492 }
```

```
BinaryOperator <col:7, col:62> 'int' '|'
|- ...
| `-BinaryOperator <col:42, col:52> 'int' '<<'
| |-ImplicitCastExpr <col:42, col:47>
| | |               'int' <IntegralCast>
| | `-ImplicitCastExpr <col:42, col:47>
| | |               'char' <LValueToRValue>
| | `-ArraySubscriptExpr <col:42, col:47>
| | |               'char' lvalue
| | |-ImplicitCastExpr <col:42>
| | | |             'char *' <ArrayToPointerDecay>
| | | `-DeclRefExpr <col:42> 'char[16]'
| | |               'buf' 'char[16]'
| | `-IntegerLiteral <col:46> 'int' 6
| `-IntegerLiteral <col:52> 'int' 8
`-ImplicitCastExpr <col:57, col:62>
  |                 'int' <IntegralCast>
  `-ImplicitCastExpr <col:57, col:62>
    |               'char' <LValueToRValue>
    `-ArraySubscriptExpr <col:57, col:62>
      |             'char' lvalue
      |-ImplicitCastExpr <col:57>
      | |           'char *' <ArrayToPointerDecay>
      | `-DeclRefExpr <col:57> 'char[16]'
      |             'buf' 'char[16]'
      `-IntegerLiteral <col:61> 'int' 7
```

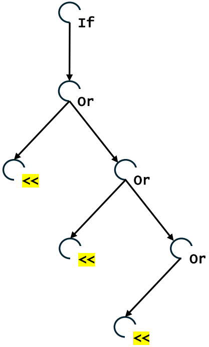
Step 2: Signature Creation

```
453 int jp2_validate(jas_stream_t *in)
454 {
455   char buf[JP2_VALIDATELEN];
...
467   if ((n = jas_stream_read(in, buf,
            JP2_VALIDATELEN)) < 0) {
468     return -1;
469   }
...
473   for (i = n - 1; i >= 0; --i) {
474     if (jas_stream_ungetc(in, buf[i]) == EOF) {
475       return -1;
476     }
477   }
...
485   if (((buf[4] << 24) | (buf[5] << 16) |
            (buf[6] << 8) | buf[7]) !=
486                       JP2_BOX_JP)
487   {
488     return -1;
489   }
...
492 }
```

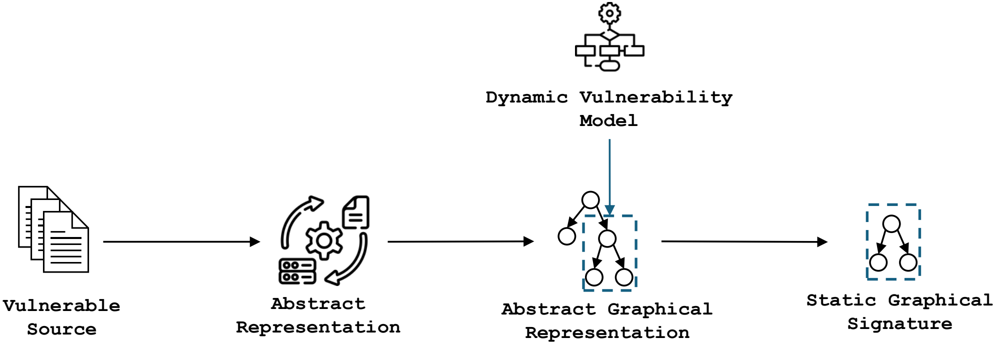


Step 2: Signature Creation

```
453 int jp2_validate(jas_stream_t *in)
454 {
455   char buf[JP2_VALIDATELEN];
...
467   if ((n = jas_stream_read(in, buf,
              JP2_VALIDATELEN)) < 0) {
468     return -1;
469   }
...
473   for (i = n - 1; i >= 0; --i) {
474     if (jas_stream_ungetc(in, buf[i]) == EOF) {
475       return -1;
476     }
477   }
...
485   if (((buf[4] << 24) | (buf[5] << 16) |
              (buf[6] << 8) | buf[7]) !=
486                     JP2_BOX_JP)
487   {
488     return -1;
489   }
...
492 }
```



Step 2: Signature Creation



Dynamic Vulnerability Model

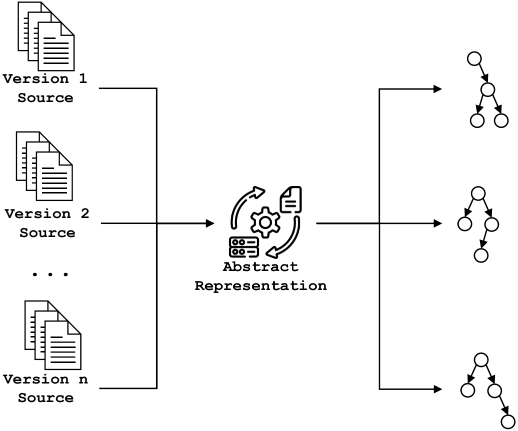
Vulnerable Source

Abstract Representation

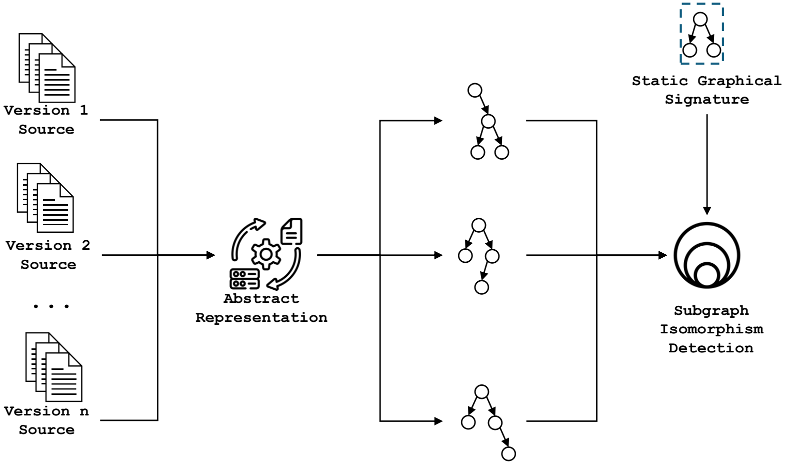
Abstract Graphical Representation

Static Graphical Signature

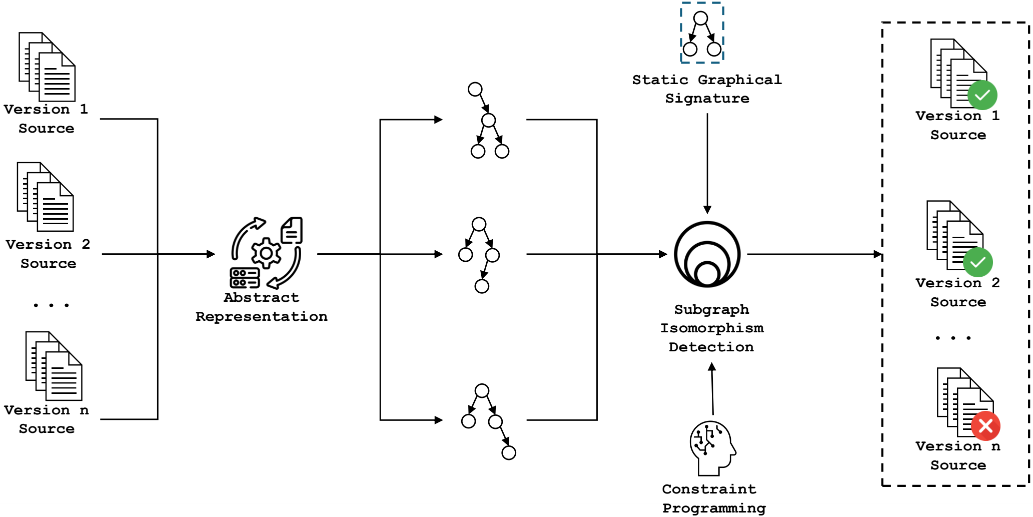
Step 3: Signature Matching



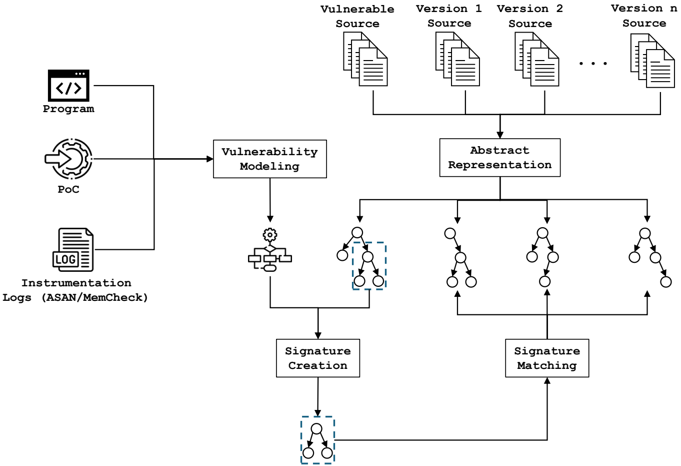
Step 3: Signature Matching



Step 3: Signature Matching



Overall Design



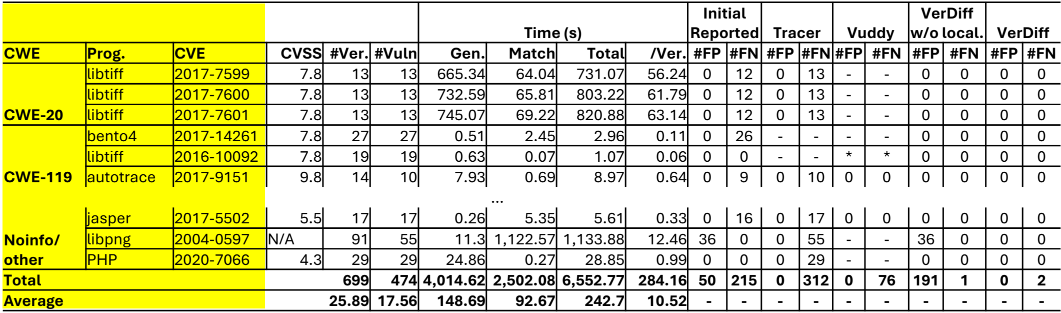
Evaluation

Dataset

CWE	Description	#CVEs	Additional
CWE-20	Improper Input Validation	9	Top 25 2023
CWE-119	Memory Buffer Misuse	80	Top 25 2023
CWE-125	Out-of-bounds Read	32	Top 25 2023
CWE-189	Numeric Errors	27	-
CWE-190	Integer Overflow	14	Top 25 2023
CWE-416	Use After Free	5	Top 25 2023
CWE-476	NULL Pointer Dereference	22	Top 25 2023
CWE-787	Out-of-bounds Write	14	Top 25 2023
CWE-noinfo	-	80	-

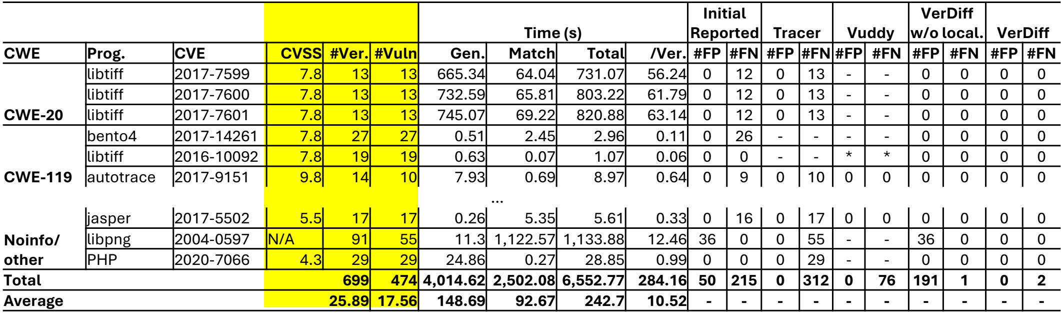
Category	Program	Used By
Graphics	autotrace	Inkscape, GIMP
	bento4	mprUI, Shaka Packager, ExoPlayer
	GraphicsMagick	Node.js, G'MIC, ImageOptim
	jasper	OpenCV, K Desktop, Copy.ai
	libpng	GIMP, Firefox, ClanLib, Chromium
	libtiff	GIMP, OpenCV, ImageMagick
Compression	openjpeg	PHP, MySQL, KDE Ark
	libzip	PHP, MySQL, KDE Ark
	zziplib	PHP, MySQL, SDL
Programming	PHP	Facebook, Wikipedia, MailChimp
	Python	Netflix, Spotify, YouTube, Instagram

VerDiff evaluates top CWEs under Linux Flaw dataset with 3+ CVEs for programs under **3 most popular** categories



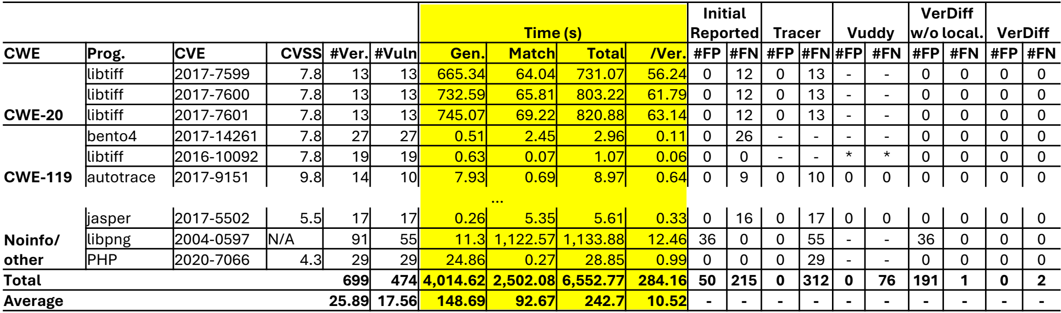
						Time (s)				Initial Reported		Tracer		Vuddy		VerDiff w/o local.		VerDiff	
CWE	**Prog.**	**CVE**	**CVSS**	**#Ver.**	**#Vuln**	**Gen.**	**Match**	**Total**	**/Ver.**	**#FP**	**#FN**	**#FP**	**#FN**	**#FP**	**#FN**	**#FP**	**#FN**	**#FP**	**#FN**
CWE-20	libtiff	2017-7599	7.8	13	13	665.34	64.04	731.07	56.24	0	12	0	13	-	-	0	0	0	0
	libtiff	2017-7600	7.8	13	13	732.59	65.81	803.22	61.79	0	12	0	13	-	-	0	0	0	0
	libtiff	2017-7601	7.8	13	13	745.07	69.22	820.88	63.14	0	12	0	13	-	-	0	0	0	0
CWE-119	bento4	2017-14261	7.8	27	27	0.51	2.45	2.96	0.11	0	26	-	-	-	-	0	0	0	0
	libtiff	2016-10092	7.8	19	19	0.63	0.07	1.07	0.06	0	0	-	-	*	*	0	0	0	0
	autotrace	2017-9151	9.8	14	10	7.93	0.69	8.97	0.64	0	9	0	10	0	0	0	0	0	0
							...												
Noinfo/ other	jasper	2017-5502	5.5	17	17	0.26	5.35	5.61	0.33	0	16	0	17	0	0	0	0	0	0
	libpng	2004-0597	N/A	91	55	11.3	1,122.57	1,133.88	12.46	36	0	0	55	-	-	36	0	0	0
	PHP	2020-7066	4.3	29	29	24.86	0.27	28.85	0.99	0	0	0	29	-	-	0	0	0	0
Total				**699**	**474**	**4,014.62**	**2,502.08**	**6,552.77**	**284.16**	**50**	**215**	**0**	**312**	**0**	**76**	**191**	**1**	**0**	**2**
Average				**25.89**	**17.56**	**148.69**	**92.67**	**242.7**	**10.52**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**

The CVEs were reported from **2004 – 2020**



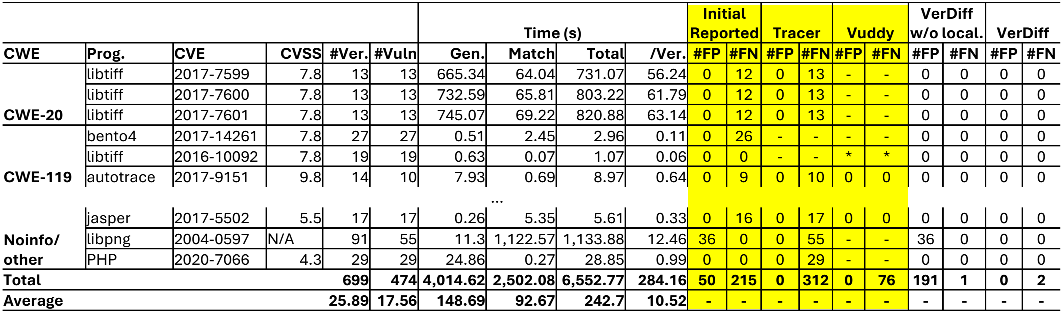
						Time (s)				Initial Reported		Tracer		Vuddy		VerDiff w/o local.		VerDiff	
CWE	**Prog.**	**CVE**	**CVSS**	**#Ver.**	**#Vuln**	**Gen.**	**Match**	**Total**	**/Ver.**	**#FP**	**#FN**	**#FP**	**#FN**	**#FP**	**#FN**	**#FP**	**#FN**	**#FP**	**#FN**
CWE-20	libtiff	2017-7599	7.8	13	13	665.34	64.04	731.07	56.24	0	12	0	13	-	-	0	0	0	0
	libtiff	2017-7600	7.8	13	13	732.59	65.81	803.22	61.79	0	12	0	13	-	-	0	0	0	0
	libtiff	2017-7601	7.8	13	13	745.07	69.22	820.88	63.14	0	12	0	13	-	-	0	0	0	0
CWE-119	bento4	2017-14261	7.8	27	27	0.51	2.45	2.96	0.11	0	26	-	-	-	-	0	0	0	0
	libtiff	2016-10092	7.8	19	19	0.63	0.07	1.07	0.06	0	0	-	-	*	*	0	0	0	0
	autotrace	2017-9151	9.8	14	10	7.93	0.69	8.97	0.64	0	9	0	10	0	0	0	0	0	0
							...												
Noinfo/ other	jasper	2017-5502	5.5	17	17	0.26	5.35	5.61	0.33	0	16	0	17	0	0	0	0	0	0
	libpng	2004-0597	N/A	91	55	11.3	1,122.57	1,133.88	12.46	36	0	0	55	-	-	36	0	0	0
	PHP	2020-7066	4.3	29	29	24.86	0.27	28.85	0.99	0	0	0	29	-	-	0	0	0	0
Total				**699**	**474**	**4,014.62**	**2,502.08**	**6,552.77**	**284.16**	**50**	**215**	**0**	**312**	**0**	**76**	**191**	**1**	**0**	**2**
Average				**25.89**	**17.56**	**148.69**	**92.67**	**242.7**	**10.52**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**

Assuming *all previous version* as vulnerable fails



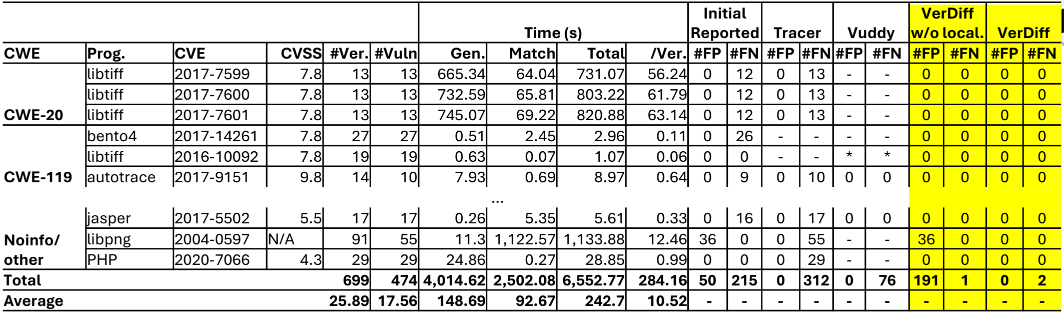
						Time (s)				Initial Reported		Tracer		Vuddy		VerDiff w/o local.		VerDiff	
CWE	**Prog.**	**CVE**	**CVSS**	**#Ver.**	**#Vuln**	**Gen.**	**Match**	**Total**	**/Ver.**	**#FP**	**#FN**	**#FP**	**#FN**	**#FP**	**#FN**	**#FP**	**#FN**	**#FP**	**#FN**
CWE-20	libtiff	2017-7599	7.8	13	13	665.34	64.04	731.07	56.24	0	12	0	13	-	-	0	0	0	0
	libtiff	2017-7600	7.8	13	13	732.59	65.81	803.22	61.79	0	12	0	13	-	-	0	0	0	0
	libtiff	2017-7601	7.8	13	13	745.07	69.22	820.88	63.14	0	12	0	13	-	-	0	0	0	0
CWE-119	bento4	2017-14261	7.8	27	27	0.51	2.45	2.96	0.11	0	26	-	-	-	-	0	0	0	0
	libtiff	2016-10092	7.8	19	19	0.63	0.07	1.07	0.06	0	0	-	-	*	*	0	0	0	0
	autotrace	2017-9151	9.8	14	10	7.93	0.69	8.97	0.64	0	9	0	10	0	0	0	0	0	0
							...												
Noinfo/ other	jasper	2017-5502	5.5	17	17	0.26	5.35	5.61	0.33	0	16	0	17	0	0	0	0	0	0
	libpng	2004-0597	N/A	91	55	11.3	1,122.57	1,133.88	12.46	36	0	0	55	-	-	36	0	0	0
	PHP	2020-7066	4.3	29	29	24.86	0.27	28.85	0.99	0	0	0	29	-	-	0	0	0	0
Total				**699**	**474**	**4,014.62**	**2,502.08**	**6,552.77**	**284.16**	**50**	**215**	**0**	**312**	**0**	**76**	**191**	**1**	**0**	**2**
Average				**25.89**	**17.56**	**148.69**	**92.67**	**242.7**	**10.52**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**

VerDiff takes <**2hr** to analyze all **699 versions**



							Time (s)			Initial Reported		Tracer		Vuddy		VerDiff w/o local.		VerDiff	
CWE	**Prog.**	**CVE**	**CVSS**	**#Ver.**	**#Vuln**	**Gen.**	**Match**	**Total**	**/Ver.**	**#FP**	**#FN**	**#FP**	**#FN**	**#FP**	**#FN**	**#FP**	**#FN**	**#FP**	**#FN**
CWE-20	libtiff	2017-7599	7.8	13	13	665.34	64.04	731.07	56.24	0	12	0	13	-	-	0	0	0	0
	libtiff	2017-7600	7.8	13	13	732.59	65.81	803.22	61.79	0	12	0	13	-	-	0	0	0	0
	libtiff	2017-7601	7.8	13	13	745.07	69.22	820.88	63.14	0	12	0	13	-	-	0	0	0	0
CWE-119	bento4	2017-14261	7.8	27	27	0.51	2.45	2.96	0.11	0	26	-	-	-	-	0	0	0	0
	libtiff	2016-10092	7.8	19	19	0.63	0.07	1.07	0.06	0	0	-	-	*	*	0	0	0	0
	autotrace	2017-9151	9.8	14	10	7.93	0.69	8.97	0.64	0	9	0	10	0	0	0	0	0	0
							...												
Noinfo/ other	jasper	2017-5502	5.5	17	17	0.26	5.35	5.61	0.33	0	16	0	17	0	0	0	0	0	0
	libpng	2004-0597	N/A	91	55	11.3	1,122.57	1,133.88	12.46	36	0	0	55	-	-	36	0	0	0
	PHP	2020-7066	4.3	29	29	24.86	0.27	28.85	0.99	0	0	0	29	-	-	0	0	0	0
Total				**699**	**474**	**4,014.62**	**2,502.08**	**6,552.77**	**284.16**	**50**	**215**	**0**	**312**	**0**	**76**	**191**	**1**	**0**	**2**
Average				**25.89**	**17.56**	**148.69**	**92.67**	**242.7**	**10.52**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**

Tracer uses **pre-existing signature** and Vuddy uses **patch based signature**

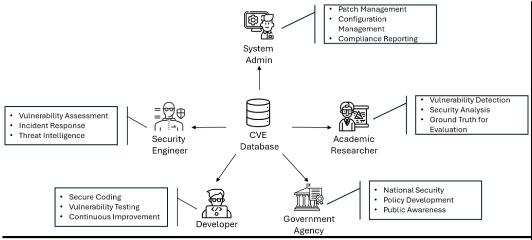


						Time (s)				Initial Reported		Tracer		Vuddy		VerDiff w/o local.		VerDiff	
CWE	**Prog.**	**CVE**	**CVSS**	**#Ver.**	**#Vuln**	**Gen.**	**Match**	**Total**	**/Ver.**	**#FP**	**#FN**	**#FP**	**#FN**	**#FP**	**#FN**	**#FP**	**#FN**	**#FP**	**#FN**
CWE-20	libtiff	2017-7599	7.8	13	13	665.34	64.04	731.07	56.24	0	12	0	13	-	-	0	0	0	0
	libtiff	2017-7600	7.8	13	13	732.59	65.81	803.22	61.79	0	12	0	13	-	-	0	0	0	0
	libtiff	2017-7601	7.8	13	13	745.07	69.22	820.88	63.14	0	12	0	13	-	-	0	0	0	0
CWE-119	bento4	2017-14261	7.8	27	27	0.51	2.45	2.96	0.11	0	26	-	-	-	-	0	0	0	0
	libtiff	2016-10092	7.8	19	19	0.63	0.07	1.07	0.06	0	0	-	-	*	*	0	0	0	0
	autotrace	2017-9151	9.8	14	10	7.93	0.69	8.97	0.64	0	9	0	10	0	0	0	0	0	0
							...												
Noinfo/ other	jasper	2017-5502	5.5	17	17	0.26	5.35	5.61	0.33	0	16	0	17	0	0	0	0	0	0
	libpng	2004-0597	N/A	91	55	11.3	1,122.57	1,133.88	12.46	36	0	0	55	-	-	36	0	0	0
	PHP	2020-7066	4.3	29	29	24.86	0.27	28.85	0.99	0	0	0	29	-	-	0	0	0	0
Total				**699**	**474**	**4,014.62**	**2,502.08**	**6,552.77**	**284.16**	**50**	**215**	**0**	**312**	**0**	**76**	**191**	**1**	**0**	**2**
Average				**25.89**	**17.56**	**148.69**	**92.67**	**242.7**	**10.52**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**

Localization narrows scope reducing FPs

Conclusion

Takeaway



System Admin

- Patch Management
- Configuration Management
- Compliance Reporting

Security Engineer

- Vulnerability Assessment
- Incident Response
- Threat Intelligence

CVE Database

Academic Researcher

- Vulnerability Detection
- Security Analysis
- Ground Truth for Evaluation

Developer

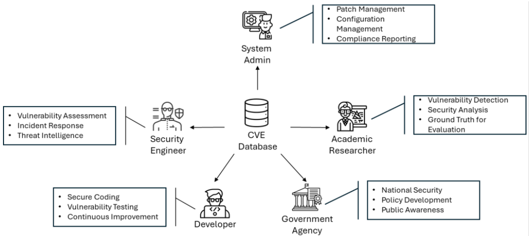
- Secure Coding
- Vulnerability Testing
- Continuous Improvement

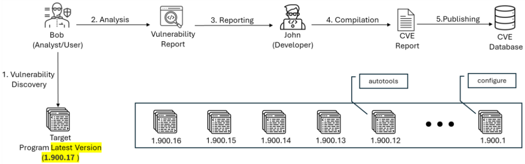
Government Agency

- National Security
- Policy Development
- Public Awareness

CVE database is a single point of ground truth

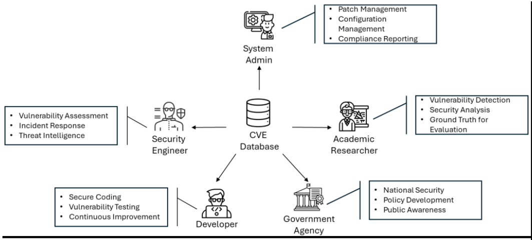
Takeaway

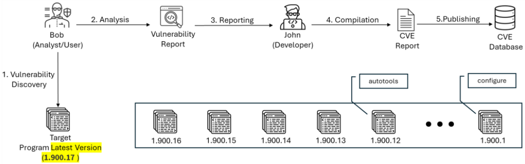


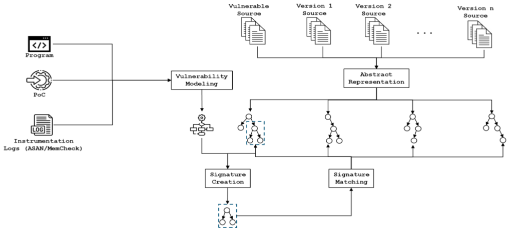


Current system prioritizes latest version creating a blind spot

Takeaway

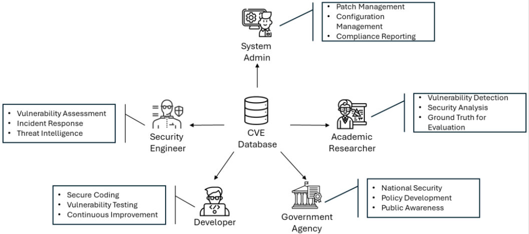


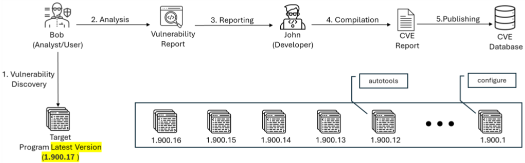


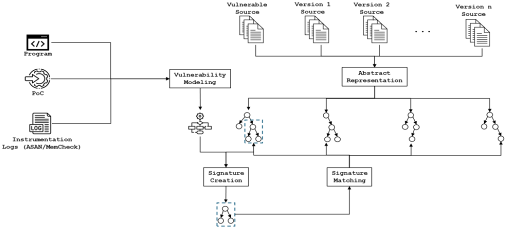


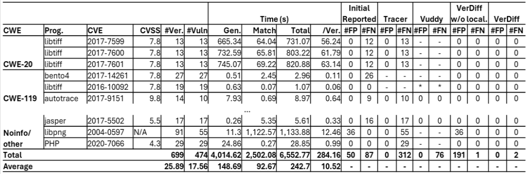
VERDIFF utilizes the information available in report to build a comprehensive report

Takeaway









						Time (s)				Initial Reported		Tracer		Vuddy		VerDiff w/o local.		VerDiff	
CWE	Prog.	CVE	CVSS	#Ver.	#Vuln	Gen.	Match	Total	/Ver.	#FP	#FN	#FP	#FN	#FP	#FN	#FP	#FN	#FP	#FN
CWE-20	libtiff	2017-7599	7.8	13	13	665.34	64.04	731.07	56.24	0	12	0	13	-	-	0	0	0	0
	libtiff	2017-7600	7.8	13	13	732.59	65.81	803.22	61.79	0	12	0	13	-	-	0	0	0	0
	libtiff	2017-7601	7.8	13	13	745.07	69.22	820.88	63.14	0	12	0	13	-	-	0	0	0	0
CWE-119	bento4	2017-14261	7.8	27	27	0.51	2.45	2.96	0.11	0	26	-	-	-	-	0	0	0	0
	libtiff	2016-10092	7.8	19	19	0.63	0.07	1.07	0.06	0	0	-	-	*	*	0	0	0	0
	autotrace	2017-9151	9.8	14	10	7.93	0.69	8.97	0.64	0	9	0	10	0	0	0	0	0	0
							...												
Noinfo/ other	jasper	2017-5502	5.5	17	17	0.26	5.35	5.61	0.33	0	16	0	17	0	0	0	0	0	0
	libpng	2004-0597	N/A	91	55	11.3	1,122.57	1,133.88	12.46	36	0	0	55	-	-	36	0	0	0
	PHP	2020-7066	4.3	29	29	24.86	0.27	28.85	0.99	0	0	0	29	-	-	0	0	0	0
Total				**699**	**474**	**4,014.62**	**2,502.08**	**6,552.77**	**284.16**	**50**	**87**	**0**	**312**	**0**	**76**	**191**	**1**	**0**	**2**
Average				**25.89**	**17.56**	**148.69**	**92.67**	**242.7**	**10.52**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**

VerDiff is evaluated against STOA tools and shows the reality of these inaccuracies

Thank you – Try VerDiff

mdsakibanwar.github.io/

hub.docker.com/r/sakibanwar/verdiff