SECTOR
BRIEFINGS
October 25-26, 2023
METRO TORONTO CONVENTION CENTRE

Ghidriff - Ghidra Binary Diffing Engine

Speaker(s): John McIntosh
@clearbluejar

ghidriff

Ghidra Binary Diffing Engine

#SecTorCA2023

whoami

- @clearbluejar
- security researcher @clearseclabs
- open source dev
- infosec blogger
- CVE North Stars

Ghidra + Binary Diffing == `ghidriff`

```
pip install ghidriff
```

```
ghidriff old.bin new.bin
```

Immediate Questions

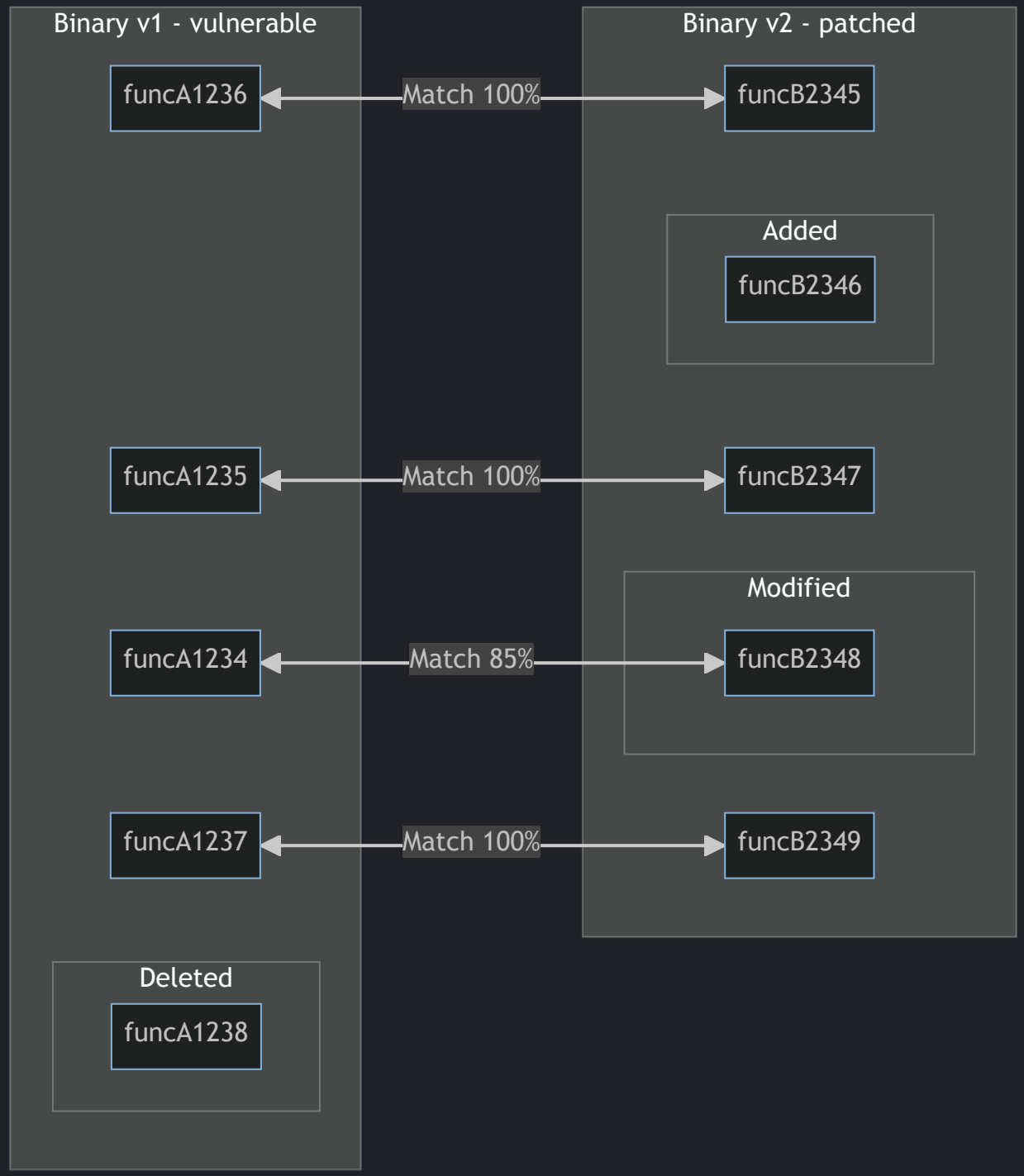
- Binary Diffing
- Ghidra
- Python
- YADT

Overview

- Binary Diffing
- Background / Motivation
- ghidriff
  - Internals
  - Features
  - CVE diffing
- Summary

Binary Diffing

What?


Binary v1 - vulnerable
Binary v2 - patched
funcA1236
Match 100%
funcB2345
Added
funcB2346
funcA1235
Match 100%
funcB2347
Modified
funcA1234
Match 85%
funcB2348
funcA1237
Match 100%
funcB2349
Deleted
funcA1238

Filter out the noise (similarities)

Focus on the signal (changes)

“ *Binary code similarity* approaches compare two or more pieces of binary code to identify their similarities and differences. ”

A Survey of Binary Code Similarity - IrfanUlHaq2019

Google

patch diffing

About 32,600,000 results (0.32 seconds)

CVE North Stars

https://cve-north-stars.github.io › docs › Patch-Diffing

Patch Diffing

Patch diffing (a specific form of binary diffing) is a technique to identify changes across versions of binaries as related to security patches. A patch ...

Table of Contents · About · Benefits · Feasibility

Why?

- **Reverse Engineering**:
  - Port previous reverse engineering work to new binary
- **Vulnerability Research**:
  - Determine if a security update actually addressed the root issue
- **Malware analysis**:
  - Find similar code in across malware samples to correlate versions of malware

Halvar Flake
@halvarflake

Follow

It's almost as if variant analysis and patch diffing is useful.

briankrebs @briankrebs · Jun 30, 2022

Google says that half of the zero day vulnerabilities it has seen exploited in the wild in the first half of 2022 are variants of previously patched vulnerabilities. And that four of the 18 0-days are variants of 2021 in-the-wild 0days. googleprojectzero.blogspot.com/2022/06/2022-0...

As of June 15, 2022, there have been 18 0-days detected and disclosed as exploited in-the-wild in 2022. When we analyzed those 0-days, we found that at least nine of the 0-days are variants of previously patched vulnerabilities. At least half of the 0-days we've seen in the first six months of 2022 could have been prevented with more comprehensive patching and regression tests. On top of that, four of the 2022 0-days are variants of 2021 in-the-wild 0-days. Just 12 months from the original in-the-wild 0-day being patched, attackers came back with a variant of the original bug.

Product	2022 ITW 0-day	Variant
Windows win32k	CVE-2022-21882	CVE-2021-1732 (2021 itw)
iOS IOMobileFrameBuffer	CVE-2022-22587	CVE-2021-30983 (2021 itw)
Windows	CVE-2022-30190 ("Follina")	CVE-2021-40444 (2021 itw)
Chromium property access interceptors	CVE-2022-1096	CVE-2016-5128 CVE-2021-30551 (2021 itw) CVE-2022-1232 (Addresses incomplete CVE-2022-1096 fix)
Chromium v8	CVE-2022-1364	CVE-2021-21195
WebKit	CVE-2022-22620 ("Zombie")	Bug was originally fixed in 2013, patch was regressed in 2016
Google Pixel	CVE-2021-39793* * While this CVE says 2021, the bug was patched and disclosed in 2022	Linux same bug in a different subsystem
Atlassian Confluence	CVE-2022-26134	CVE-2021-26084
Windows	CVE-2022-26925 ("PetitPotam")	CVE-2021-36942 (Patch regressed)

So, what does this mean?

10:20 AM · Jun 30, 2022

How?

How can I perform a patch diff?

Searching for: **how to perform a patch diff**

Generating answers for you…

To perform a patch diff, you need to have two copies of the code: one with your changes and one without. Then you can use the **diff** command to compare them and generate a patch file. For example, if you want to create a patch for a single file, you can use this command [1] [2]:

```
diff -u original.c new.c > original.patch
```

This will create a patch file named original.patch that contains the differences between original.c and new.c in the unified format.

To apply the patch to another file, you can use the **patch** command. For example, if you want to apply the patch to a file named old.c, you can use this command [1] [3]:

```
patch old.c < original.patch
```

This will modify old.c with the changes from original.patch.

To undo a patch, you can use the **-R** option with the patch command. For example, if you want to revert the changes made to old.c by original.patch, you can use this command [1] [2]:

```
patch -R old.c < original.patch
```

This will restore old.c to its original state before applying the patch.

Learn more: 1. shellhacks.com 2. stephenjungels.com 3. pair.com 4. stackoverflow.com

2 of 20

72 Ghidra/Features/Decompiler/ghidra_scripts/classrecovery/RTTIGccClassRecoverer.java

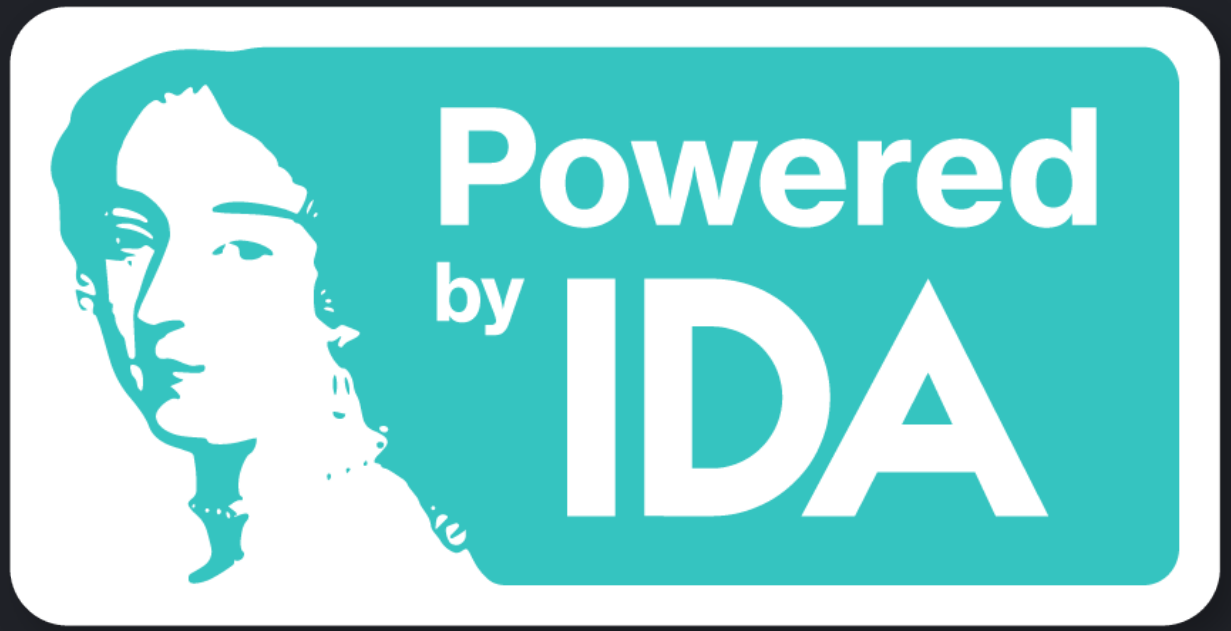
```diff
@@ -17,7 +17,14 @@
 package classrecovery;

 import java.io.UnsupportedEncodingException;
- import java.util.*;
+ import java.util.ArrayList;
+ import java.util.Collection;
+ import java.util.HashMap;
+ import java.util.HashSet;
+ import java.util.Iterator;
+ import java.util.List;
+ import java.util.Map;
+ import java.util.Set;

 import ghidra.app.cmd.label.DemanglerCmd;
 import ghidra.app.plugin.core.analysis.ReferenceAddressPair;
@@ -26,20 +33,67 @@
 import ghidra.app.util.demangler.DemanglerUtil;
 import ghidra.framework.plugintool.PluginTool;
 import ghidra.program.flatapi.FlatProgramAPI;
- import ghidra.program.model.address.*;
- import ghidra.program.model.data.*;
+ import ghidra.program.model.address.Address;
+ import ghidra.program.model.address.AddressIterator;
+ import ghidra.program.model.address.AddressOutOfBoundsException;
+ import ghidra.program.model.address.AddressRange;
+ import ghidra.program.model.address.AddressRangeIterator;
+ import ghidra.program.model.address.AddressSet;
+ import ghidra.program.model.address.AddressSetView;
+ import ghidra.program.model.data.ArrayDataType;
+ import ghidra.program.model.data.CategoryPath;
+ import ghidra.program.model.data.CharDataType;
+ import ghidra.program.model.data.DataType;
+ import ghidra.program.model.data.DataTypeComponent;
+ import ghidra.program.model.data.DataTypeConflictHandler;
+ import ghidra.program.model.data.DataUtilities;
```

But we don't have text...

bins > fxsroute.dll.x64.10.0.22000.856

```
          00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded Text
00000000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  M Z . . . . . . . . . . . . . .
00000010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  . . . . . . . . @ . . . . . . .
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  . . . . . . . . . . . . . . . .
00000030  00 00 00 00 00 00 00 00 00 00 00 00 E8 00 00 00  . . . . . . . . . . . . . . . .
00000040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  . . . . . . . . ! . . L . ! T h
00000050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  i s   p r o g r a m   c a n n o
00000060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t   b e   r u n   i n   D O S
00000070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  m o d e . . . . $ . . . . . . .
00000080  CE 09 81 30 8A 68 EF 63 8A 68 EF 63 8A 68 EF 63  . . . 0 . h . c . h . c . h . c
00000090  59 1A EB 62 87 68 EF 63 59 1A EC 62 8E 68 EF 63  Y . . b . h . c Y . . b . h . c
000000A0  8A 68 EE 63 65 68 EF 63 59 1A EE 62 97 68 EF 63  . h . c e h . c Y . . b . h . c
000000B0  59 1A EF 62 8B 68 EF 63 59 1A E7 62 90 68 EF 63  Y . . b . h . c Y . . b . h . c
000000C0  59 1A EA 62 83 68 EF 63 59 1A 10 63 8B 68 EF 63  Y . . b . h . c Y . . c . h . c
000000D0  59 1A ED 62 8B 68 EF 63 52 69 63 68 8A 68 EF 63  Y . . b . h . c R i c h . h . c
000000E0  00 00 00 00 00 00 00 00 50 45 00 00 64 86 06 00  . . . . . . . . P E . . d . . .
000000F0  8E 71 C4 DC 00 00 00 00 00 00 00 00 F0 00 22 20  . q . . . . . . . . . . . . " 
```

fortunately...


Powered
by
IDA

android > com.whatsapp_2.19.133.arm64-v8a.libwhatsapp.so

```
          00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded Text
00000000  7F 45 4C 46 02 01 01 00 00 00 00 00 00 00 00 00  . E L F . . . . . . . . . . . .
00000010  03 00 B7 00 01 00 00 00 D0 E5 02 00 00 00 00 00  . . . . . . . . . . . . . . . .
00000020  40 00 00 00 00 00 00 00 A8 E3 52 00 00 00 00 00  @ . . . . . . . . . R . . . . .
00000030  00 00 00 00 40 00 38 00 08 00 40 00 19 00 18 00  . . . . @ . 8 . . . @ . . . . .
00000040  01 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00  . . . . . . . . . . . . . . . .
00000050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  . . . . . . . . . . . . . . . .
00000060  78 2B 51 00 00 00 00 00 78 2B 51 00 00 00 00 00  x + Q . . . . . x + Q . . . . .
00000070  00 00 01 00 00 00 00 00 01 00 00 00 06 00 00 00  . . . . . . . . . . . . . . . .
00000080  70 37 51 00 00 00 00 00 70 37 52 00 00 00 00 00  p 7 Q . . . . . p 7 R . . . . .
00000090  70 37 52 00 00 00 00 00 10 AA 01 00 00 00 00 00  p 7 R . . . . . . . . . . . . .
000000A0  A0 CB 10 00 00 00 00 00 00 00 01 00 00 00 00 00  . . . . . . . . . . . . . . . .
000000B0  02 00 00 00 06 00 00 00 58 BE 51 00 00 00 00 00  . . . . . . . . X . Q . . . . .
000000C0  58 BE 52 00 00 00 00 00 58 BE 52 00 00 00 00 00  X . R . . . . . X . R . . . . .
000000D0  70 02 00 00 00 00 00 00 70 02 00 00 00 00 00 00  p . . . . . . . p . . . . . . .
000000E0  08 00 00 00 00 00 00 00 04 00 00 00 04 00 00 00  . . . . . . . . . . . . . . . .
000000F0  00 02 00 00 00 00 00 00 00 02 00 00 00 00 00 00  . . . . . . . . . . . . . . . .
```

Listing: ntkrnlmp.exe.x64.10.0.22000.2416

```
                                                                    0
 ***********************************************
 *                    FUNCTION                 *
 ***********************************************
      DifIoCreateFileWrapper        XREF…1401005a4(*),
                                        14015de70(*)
14060c810 48 8b c4                  MOV            RAX,RSP
14060c813 48 89 58 08               MOV            qword ptr [RAX + …
14060c817 48 89 70 10               MOV            qword ptr [RAX + …
14060c81b 48 89 78 18               MOV            qword ptr [RAX + …
14060c81f 55                        PUSH           RBP
14060c820 41 54                     PUSH           R12
14060c822 41 55                     PUSH           R13
14060c824 41 56                     PUSH           R14
14060c826 41 57                     PUSH           R15
14060c828 48 8d 68 d1               LEA            RBP,[RAX + -0x2f]
14060c82c 48 81 ec e0 00 00 00      SUB            RSP,0xe0
14060c833 44 8b e2                  MOV            R12D,EDX
14060c836 4d 8b f8                  MOV            R15,R8
14060c839 33 d2                     XOR            EDX,EDX
14060c83b 4c 8b e9                  MOV            R13,RCX
14060c83e 48 8d 4d 97               LEA            RCX,[RBP + -0x69]
14060c842 4d 8b f1                  MOV            R14,R9
14060c845 44 8d 42 68               LEA            R8D,[RDX + 0x68]
14060c849 e8 32 6b e2 ff            CALL           memset          undefined me…
```

Decompile: DifloCreateFileWrapper - (ntkrnlmp.exe.x64.10.0.22000.2416)

```
65   uStack_48 = param_2;
66   uStack_40 = param_1;
67   for (puVar4 = *(undefined8 **)(undefined8 *)(lVar1 + 0x20); puVar4 != (undefined8 *)(lVar1 + 0x20)
68       ; puVar4 = (undefined8 *)*puVar4) {
69     if (puVar4 != (undefined8 *)0x10) {
70       _guard_dispatch_icall(&uStack_98);
71     }
72   }
73 LAB_14060c935:
74   uVar3 = IoCreateFile(param_1,param_2,param_3,param_4,param_5,param_6,param_7,param_8,param_9,
75                        param_10,param_11,param_12,param_13,param_14);
76   uStack_38 = (uint)uVar3;
77   if (lVar1 != 0) {
78     pplVar6 = (longlong **)(lVar1 + 0x30);
79     pplVar5 = (longlong **)*pplVar6;
80     if (pplVar5 != pplVar6) {
81       do {
82         if (pplVar5 != (longlong **)0x10) {
83           _guard_dispatch_icall(&uStack_98);
84         }
85         pplVar5 = (longlong **)*pplVar5;
86       } while (pplVar5 != pplVar6);
87       uVar3 = (ulonglong)uStack_38;
88     }
89   }
90   return uVar3;
91 }
```

Edit Help

Function Call Graph [Version Tracking (SOURCE TOOL): CVE-2022-36934:/com.whatsapp.2.22.16.11/libwhatsapp.so]

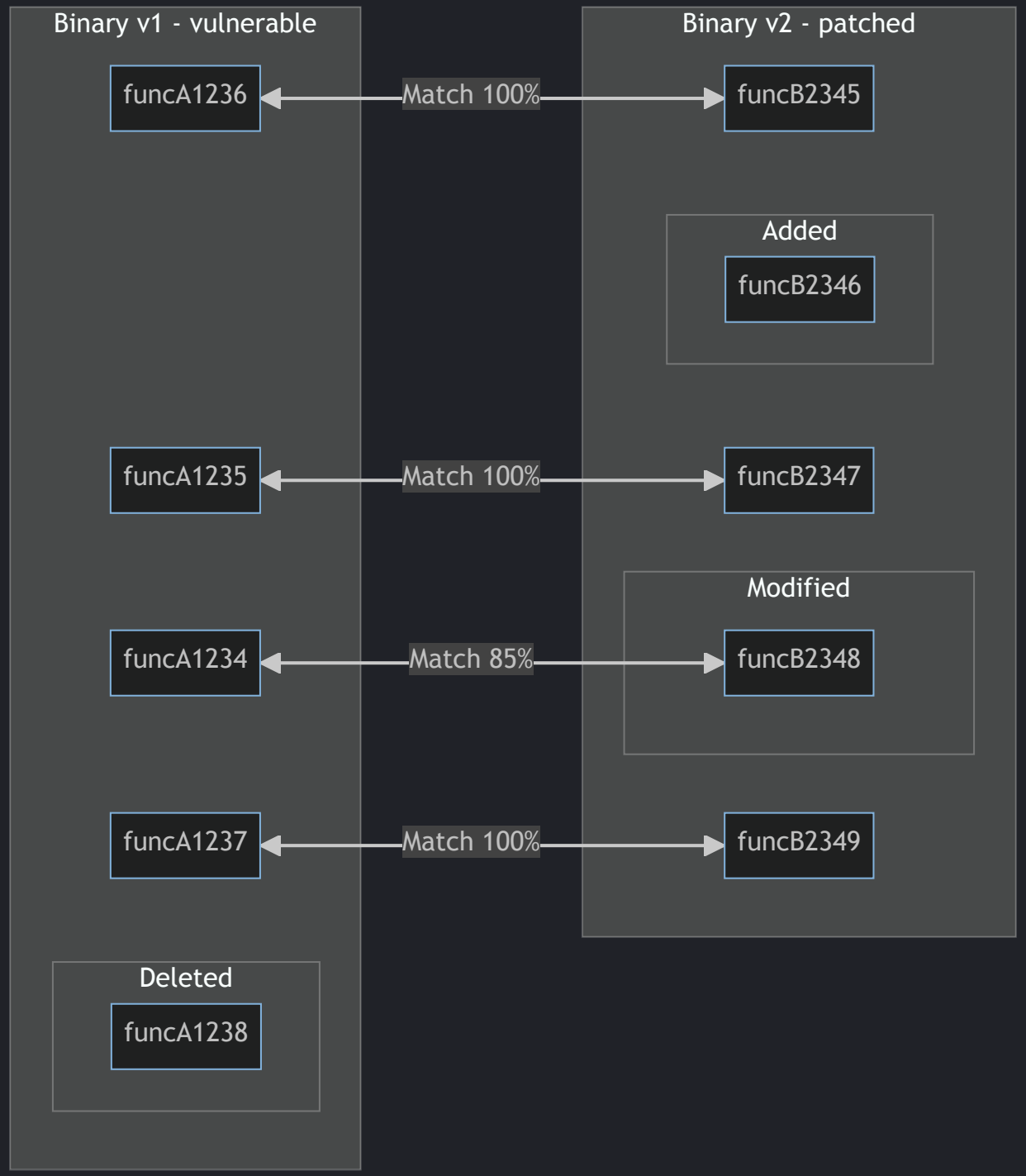
Function Call Graph - FUN_006470cc (450 functions; 1572 edges)

SRE tools distill binaries into objects and relationships that we can compare

Diffing Tools

Purpose

Find the *added*, *deleted*, and *modified* functions and data between two binaries.



Complexity

Assymetry

> It takes relatively little work to change source code and recompile, while the analysis of the object code will have to be completely redone to detect the changes.

Structural Comparison of Executable Objects

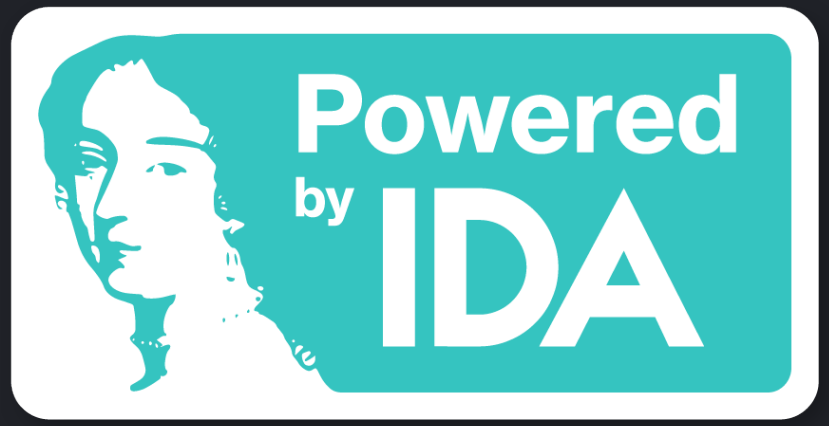
Small source change and greatly impact complied binary:

1. Registers used to hold specific variables (using RAX instead of RDX)
2. Basic block arrangement and branches (flowgraph and callgraph respectively)
3. Compiler might optimize instructions that perform the same operations (`xor eax, eax` or `mov eax,0`)

Each diffing tool attempts to **bring symmetry** to the assymetric problem of REing binaries

Binary Diffing Tool Options


BinDiff


Powered
by
IDA

BinDiff

Diff, Navigate, Audit

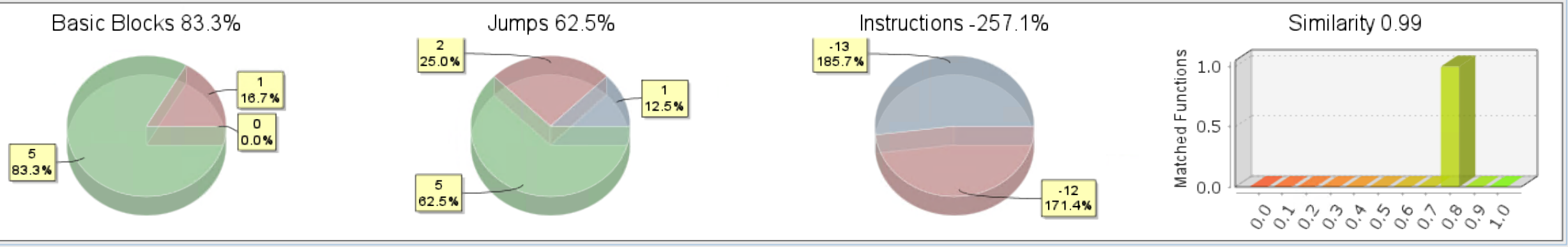
Three applications of graphs and graphing for security

Halvar Flake – Blackhat Briefings Las Vegas 2004

“In 2004, I started a company called zynamics... One of our products (BinDiff) became an industry standard and even a verb...”

Halver Flake

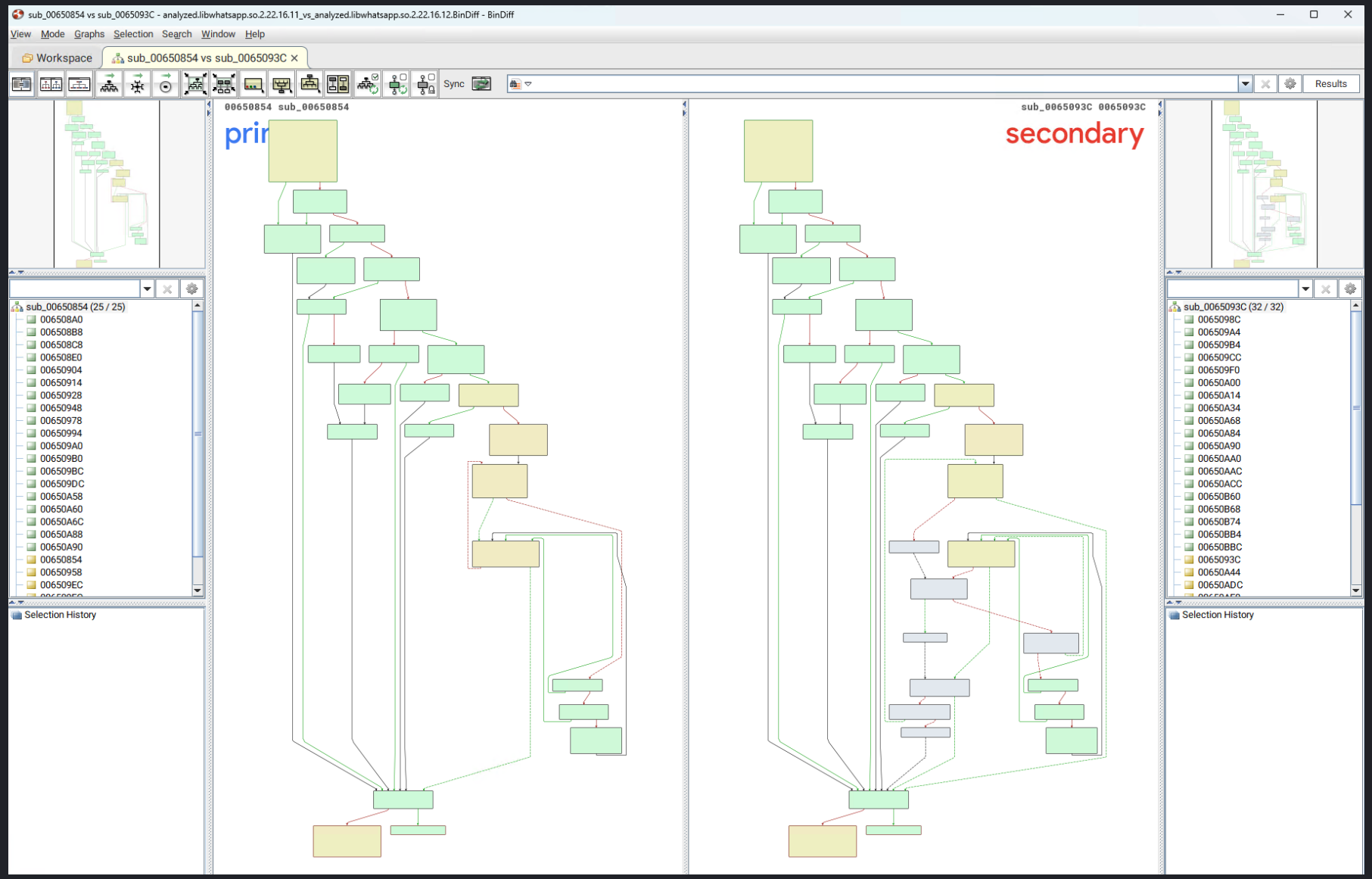
Overview



32856 / 32856 Matched Functions

Show structural changes | Show only instructions changed | Show identical

Similarity	Confidence	Address	Primary Name	Type	Address	Secondary Name	Type	Basic Blocks	Jumps
0.33	0.50	000000...	NtTranslateFilePath$filt$0	Normal	000000...	NtTranslateFilePath$filt$0	Normal	1 1 0	
0.38	0.73	000000...	ExpKdPullRemoteFileForU...	Normal	000000...	ExpKdPullRemoteFileForU...	Normal	0 1 2	2
0.42	0.73	000000...	KiVerifyXcpt10fin1	Normal	000000...	KiVerifyXcpt10fin1	Normal	0 1 1	1
0.42	0.73	000000...	NtEnumerateBootEntries$...	Normal	000000...	NtEnumerateBootEntries$...	Normal	1 1 0	1
0.44	0.73	000000...	CmQueryFeatureConfigurat...	Normal	000000...	CmQueryFeatureConfigurat...	Normal	1 1 0	1
0.75	0.99	000000...	SPCallServerHandleClepKdf	Normal	000000...	SPCallServerHandleClepKdf	Normal	11 12 0	20 20 0
0.83	0.99	000000...	MiPreserveBootDecisions	Normal	000000...	MiPreserveBootDecisions	Normal	10 30 0	23 41 6
0.85	0.95	000000...	HalpMiscGetParameters	Normal	000000...	HalpMiscGetParameters	Normal	2 66 10	16 92 30
0.87	**0.99**	**000000...**	**KiVerifyXcpt2fin0**	**Normal**	**000000...**	**KiVerifyXcpt2fin0**	**Normal**	**1 5 0**	**2 5 1**
0.89	0.99	000000...	KeQuerySpeculationContro...	Normal	000000...	KeQuerySpeculationContro...	Normal	0 33 11	3 48 20
0.89	0.97	000000...	WritePartitionTable	Normal	000000...	WritePartitionTable	Normal	4 59 3	24 74 25
0.96	0.99	000000...	KiDetectHardwareSpecCon...	Normal	000000...	KiDetectHardwareSpecCon...	Normal	0 80 3	8 117 12
0.99	0.99	000000...	CmRenameKey	Normal	000000...	CmRenameKey	Normal	0 292 1	7 481 8
0.99	0.99	000000...	Phase1InitializationDiscard	Normal	000000...	Phase1InitializationDiscard	Normal	1 213 0	2 336 1
1.00	0.99	000000...	HvlQueryActiveHypervisor...	Normal	000000...	HvlQueryActiveHypervisor...	Normal	0 3 0	0 2 0
1.00	0.99	000000...	CmpTraceHiveSaveStop	Normal	000000...	CmpTraceHiveSaveStop	Normal	0 3 0	0 4 0
1.00	0.99	000000...	IoIsActivityTracingEnabled	Normal	000000...	IoIsActivityTracingEnabled	Normal	0 4 0	0 4 0


sub_00650854 vs sub_0065093C - analyzed.libwhatsapp.so.2.22.16.11_vs_analyzed.libwhatsapp.so.2.22.16.12.BinDiff - BinDiff
View Mode Graphs Selection Search Window Help
Workspace
sub_00650854 vs sub_0065093C
Sync
Results
00650854 sub_00650854
prir
sub_0065093C 0065093C
secondary
sub_00650854 (25 / 25)
006508A0
006508B8
006508C8
006508E0
00650904
00650914
00650928
00650948
00650978
00650994
006509A0
006509B0
006509BC
006509DC
00650A58
00650A60
00650A6C
00650A88
00650A90
00650854
00650958
006509EC
Selection History
sub_0065093C (32 / 32)
0065098C
006509A4
006509B4
006509CC
006509F0
00650A00
00650A14
00650A34
00650A68
00650A84
00650A90
00650AA0
00650AAC
00650ACC
00650B60
00650B68
00650B74
00650BB4
00650BBC
0065093C
00650A44
00650ADC
Selection History

```
00650854    sub_00650854
00650A1C    ldr       x0, [x25]
00650A20    add       w21, w21, #0x1
00650A24    bl        FUN_0067c8cc
00650A28    cmp       w21, w0, UXTB
00650A2C    mov       w20, wzr
00650A30    b.cs      LAB_00650948
```

```
0065093C    sub_0065093C

00650B30    add       w25, w28, #0x1

00650B34    tbz       w28, #0x1f, LAB_00650b94
```

BinDiff

- The matching is good
- The UI for highlighting changes between the two functions is clear and obvious
- It is not obvious though which changes in the matched functions list may be important
- No support for decompiler
- UI is outside of IDA
- Seems to not get caught by name changes, offset changes, etc.

Google

Maddie Stone 2019 Whats Up With WhatsApp @Google

Diaphora

README.md

Diaphora (διαφορά, Greek for 'difference') version 3.0 is the most advanced program diffing tool (working as an IDA plugin) available as of today (2023). It was released first during SyScan 2015 and has been actively maintained since this year: it has been ported to every single minor version of IDA since 6.8 to 8.3.

IDA ... | Best m... | Partial m... | Diff pseudo-code sub_8D3C - luaopen_evs... | Unreliable m... | Unmatched in ...

Line	Address	Name	Address 2	Name 2	Ratio	BBlo	BBlc	Description
00035	00008e50	sub_8E50	000002fc	luaf_evsocket_min_rbuf	0.930	1	1	Mnemonics small-primes-product
00031	0000c0b4	sub_C0B4	00000174	luaf_evsocket_start	0.880	1	1	Mnemonics small-primes-product
00032	0000c28c	sub_C28C	00000194	luaf_evsocket_stop	0.880	1	1	Mnemonics small-primes-product
00037	00008d3c	sub_8D3C	00000060	luaopen_evsocketlib	0.870	1	1	Mnemonics small-primes-product
00036	000093c0	sub_93C0	00000850	luaf_evsocket_str2ip	0.830	7	7	Mnemonics small-primes-product
00034	00009314	sub_9314	00000794	luaf_evsocket_now	0.730	1	1	Mnemonics small-primes-product
00030	00047984	sub_47984	00000d40	luaf_evsocket_new_tcpfd	0.670	2	1	Mnemonics small-primes-product
00033	0009aa00	sigemptyset	00000968	lua_evsocket_udp_recvfrom_r...	0.620	1	1	Mnemonics small-primes-product
00029								
00000								
00001								
00002								
00003								

IDA ... | Best m... | Partial m... | Diff pseudo-code sub_8D3C - luaopen_evs... | Unreliable m... | Unmatched in ...

```
n1 signed int __fastcall sub_8D3C(int a1, int a2)
 2 {
n3   _DWORD *v2; // r4@1
 4   int v3; // r1@1
 5
t6   v2 = (_DWORD *)a1;
 7   luaL_checkversion_((_DWORD *)a1, a2, 1082093568, 0, 72);
 8   lua_createtable((int)v2, 0, 17);
 9   luaL_setfuncs((int)v2, (int *)&off_A1EF0, 0);
10   luaL_newmetatable((int)v2, (int)"evs");
11   luaL_checkversion_(v2, v3, 1082093568, 0, 72);
12   lua_createtable((int)v2, 0, 10);
13   luaL_setfuncs((int)v2, (int *)&off_A1F80, 0);
14   lua_setfield((int)v2, -2, (int)"__index");
15   hooknames_2682((int)v2, (int)"__gc");
16   lua_pushcclosure(v2, (int)sub_C0B4, 0);
17   sub_FFC8((int)v2, -3);
18   lua_settop((int)v2, -2);
19   luaL_newmetatable((int)v2, (int)"evs_ssl_c");
20   lua_settop((int)v2, -2);
21   return 1;
22 }
```

```
n1 signed int __fastcall luaopen_evsocketlib(int a1)
 2 {
n
 3   int v1; // r4@1
 4
t5   v1 = a1;
 6   luaL_checkversion_(a1);
 7   lua_createtable(v1, 0, 17);
 8   luaL_setfuncs(v1, &luaevsocket_lib_constructor, 0);
 9   luaL_newmetatable(v1, &unk_129C);
10   luaL_checkversion_(v1);
11   lua_createtable(v1, 0, 13);
12   luaL_setfuncs(v1, &luaevsocket_lib, 0);
13   lua_setfield(v1, -2, "__index");
14   lua_pushstring(v1, "__gc");
15   lua_pushcclosure(v1, luaf_evsocket_close, 0);
16   lua_settable(v1, -3);
17   lua_settop(v1, -2);
18   luaL_newmetatable(v1, "evs_ssl_c");
19   lua_settop(v1, -2);
20   return 1;
21 }
```

Legends

Colors	Links
Added	(f)irst
Changed	change
Deleted	(n)ext change
	(t)op

Diaphora

- Matching wasn't great
- Tends to get thrown off by naming, different offsets, etc.
- Has support for decompilation diffing, but rather basic
- Open source and currently developed!
- Integrated fully into IDA with support coming for other tools

Google

Maddie Stone 2019 Whats Up With WhatsApp @Google

Popular and recent release looks to provide a ton of new features

Diaphora 3.0

MISC: Increased Diaphora version to 3.0.0.
API: Add support for the fist 'to be exposed' function, used to get the callgraph percent difference.
CONFIG: Added multiple configuration options in diaphora_config.py.
CORE: Added CodeCut support to find anonymous compilation units.
CORE: Added IDAMagicStrings to try to find compilation unit names.
CORE: Added support to enable/disable exporting microcode.
CORE: Added support to find and export Compilation Units.
CORE: By default, run a helper script that tries to find potentially fixed vulnerabilities when a patch diffing session
function names is detected.
CORE: Coallesce contiguous named compilation units using the minimum and maximum address.
CORE: Do not directly add matches to choosers, instead, work with internal Python dict objects and process them
the diffing session is done.
CORE: More refactorizations for properly supporting multimatches and finding the best matches.
CORE: Set a name to compilation units when enough matches indicate the name of the compilation unit using
IDAMagicStrings.
DATABASE: Added proper indices and fine tunning of SQL heuristics and queries.
DATABASE: Moved tables and indices definitions to a different file.
DIFF: Support for handling mutiple matches by showing them in a different chooser.
DOC: Documented all functions and members in diaphora.py.
EXPORT: Add the `func_id` field to the `instructions` table.
EXPORT: Consider data references to functions from functions also code references.
GUI: Add support for Python logging facilities.
GUI: Add support for diffing microcode assembly.
GUI: Add support to "Diff microcode in a graph".
GUI: Added environment variable DIAPHORA_LOG_PRINT to print to stdout instead of using Python logging facilit
GUI: Added initial support to view callers and callees of functions matches.
GUI: Added microcode related configuration options and updated a bit the main dialogue.
GUI: Added support to configure colors for diffing and call graph viewing.
GUI: Enable, by default, slow heuristics only for databases of ~1,000 functions at much.
GUI: Renamed 'Experimental' to 'Enable Speed Ups', as the old 'experimental' heuristics are either upgraded to 'n
or removed.
HEUR: Add a filter for a minimum of 3 instructions for heuristic 'Same address, nodes, edges and mnemonics'.
HEUR: Add support for speed ups (internally called 'dirty heuristics') for detected symbols stripped matching and
diffing.

Version Tracking Tool


CALLED A "PIECE OF JUNK" AND A "BUCKET OF BOLTS"
STILL SAVES EVERYONE'S ASS AT THE END OF ALL THREE MOVIES

Version Tracking: CVE-2020-1048-Session1

File Edit Window Help

Version Tracking Matches - [Session: CVE-2020-1048-Session1] - 16997 matches (of 22395)

Tag	Sessio...	Status	Type	Score	Confidenc...	Votes	# Con...	Multipl...	Source Namespace	Source Label	Source Addr...	Multipl...	Dest Namesp...	Dest Label	Dest Address	Source Length	Dest Le...	Algorithm
	14		Function	1.000	2.332	1	0		Global	GetClientTokenForNotification	7ff76f1d2c4		Global	GetClientTokenF...	7ff76f1d344	63	63	Combined Functi...
	14		Function	1.000	2.983	1	0	2	Global	IrdaDisconnect	7ff76f9a054	2	Global	IrdaDisconnect	7ff76f9a2d4	167	167	Combined Functi...
	14		Function	1.000	3.702	1	0	2	Global	SplOpenPrinter	7ff76f02218	2	Global	SplOpenPrinter	7ff76f02210	2545	2545	Combined Functi...
	14		Function	1.000	3.125	1	6	3	THashTreeConta...	THashTreeContainer<class_...	7ff76f0c934	3	THashTreeCo...	THashTreeConta...	7ff76f0cae0	251	251	Combined Functi...
	14		Function	0.955	2.643	4	0		Global	CreateDirectoryWithoutImp...	7ff76f5c530		Global	CreateDirectory...	7ff76f5c6e0	147	147	Combined Functi...
	14		Function	1.000	2.979	1	0	2	NPackageInstallL...	Initialize	7ff76f0baf0	2	NPackageIns...	Initialize	7ff76f0bb2c	315	315	Combined Functi...
	14		Function	1.000	3.009	5	0	2	Global	GetGUID	7ff76f845b0	2	Global	GetGUID	7ff76f84734	176	176	Combined Functi...
	14		Function	1.000	2.247	3	0	2	NCoreLibrary	EasyRelease	7ff76f1a350	2	NCoreLibrary	EasyRelease	7ff76f1a3e0	29	29	Combined Functi...
	14		Function	1.000	2.557	21	0		Global	FindSpoolerByNameDecRef	7ff76f04390		Global	FindSpoolerByNa...	7ff76f04374	81	81	Combined Functi...
	14		Function	1.000	2.804	1	0	2	NPackageInstallL...	RegisterVerifyWorker	7ff76f0bd2c	2	NPackageIns...	RegisterVerifyW...	7ff76f0bd70	47	47	Combined Functi...
	14		Function	1.000	2.614	1	0	2	Global	SplIsValidDevmode<struct_...	7ff76f9c8e0	2	Global	SplIsValidDevm...	7ff76f9cb40	77	77	Combined Functi...
	14		Function	1.000	2.166	0	0	2	NAsyncNotifyLoc...	UnregisterForNotifications`a...	7ff76fa6184	2	NAsyncNotify...	UnregisterForNo...	7ff76fa63d4	9	9	Combined Functi...
	14		Function	1.000	2.955	1	0		Global	StrCatPrefixMsz	7ff76f61670		Global	StrCatPrefixMsz	7ff76f617d8	376	376	Combined Functi...
	14		Function	0.989	2.782	1	0	2	Global	SpoolerTraceEventWrite	7ff76f9e03c	2	Global	SpoolerTraceEv...	7ff76f9e290	250	250	Combined Functi...
	14		Function	1.000	2.929	2	0	2	Global	CheckDriverAttributes	7ff76f1cfa0	2	Global	CheckDriverAttr...	7ff76f1d024	321	321	Combined Functi...
	14		Function	1.000	2.225	4	138		Global	__imp_load_WSAStartup	7ff76f19c34		Global	__imp_load_WS...	7ff76f19cc4	12	12	Combined Functi...
	14		Function	1.000	2.855	1	0	2	Global	CreateFilePool	7ff76f153d8	2	Global	CreateFilePool	7ff76f15420	434	434	Combined Functi...
	14		Function	1.000	2.317	2	0	2	NCOMLibrary::C...	~ComLeakCleaner	7ff76f2a8fc	2	NCOMLibrary...	~ComLeakClean...	7ff76f2a9c0	2	2	Combined Functi...

Filter: | Score Filter: 0.000 to 1.000 | Confidence Filter: -9.999 to 9.999 | Length Filter: 0

Version Tracking Functions - [Session: CVE-2020-1048-Session1] - Source Functions - 2479 functions / Destination Functions - 2493 functions

Source = WindowsPrintSpooler:/2020-04/p..ooler-core-localspl_6.1.7601.24383/localspl.dll

Label	Location	Function Signature
FUN_7ff76f01010	7ff76f01010	undefined FUN_7ff76f01010(int param_1, ...
TEventWrite_Msg	7ff76f010e0	void TEventWrite_Msg(ulong param_1, ush...
LeaveSplSem	7ff76f010ec	undefined LeaveSplSem(undefined8 param_...
FUN_7ff76f01110	7ff76f01110	undefined FUN_7ff76f01110(undefined8 pa...
EnterSplSem	7ff76f011b4	undefined EnterSplSem(int param_1, usho...
__security_check_cookie	7ff76f011e0	void __security_check_cookie(uintptr_t ...
FindSpoolerByName	7ff76f01240	ushort * FindSpoolerByName(LPCWSTR para...
GetTokenHandle	7ff76f012b0	undefined8 GetTokenHandle(undefined8 pa...
FUN_7ff76f01344	7ff76f01344	undefined FUN_7ff76f01344(void * param_...
GetPrinterSize	7ff76f0159c	uint GetPrinterSize(longlong param_1, i...
GetPrinterPorts	7ff76f017cc	undefined GetPrinterPorts(longlong para...

Filter:

Destination = WindowsPrintSpooler:/2020-05/p..ooler-core-localspl_6.1.7601.24554/localspl.dll

Label	Location	Function Signature
FUN_7ff76f01010	7ff76f01010	undefined FUN_7ff76f01010(int param_1, ...
TEventWrite_Msg	7ff76f010e0	void TEventWrite_Msg(ulong param_1, ush...
LeaveSplSem	7ff76f010f0	undefined LeaveSplSem(undefined8 param_...
FUN_7ff76f01114	7ff76f01114	undefined FUN_7ff76f01114(undefined8 pa...
EnterSplSem	7ff76f011b8	undefined EnterSplSem(int param_1, usho...
__security_check_cookie	7ff76f011e0	void __security_check_cookie(uintptr_t ...
FindSpoolerByName	7ff76f01240	ushort * FindSpoolerByName(LPCWSTR para...
GetTokenHandle	7ff76f012b0	undefined8 GetTokenHandle(undefined8 pa...
FUN_7ff76f01344	7ff76f01344	undefined FUN_7ff76f01344(void * param_...
GetPrinterSize	7ff76f0159c	uint GetPrinterSize(longlong param_1, i...
GetPrinterPorts	7ff76f017cc	undefined GetPrinterPorts(longlong para...

Filter:

A match already exists between TEventWrite_Msg and TEventWrite_Msg.

Decompile View | Listing View

Source: **TEventWrite_Msg()** in /2020-04/p..ooler-core-localspl_6.1.7601.24383/localspl.dll

```
                    **************************************************************
                    * void __cdecl TEventWrite_Msg(unsigned long,unsigned sho... *
                    **************************************************************
                    void __fastcall TEventWrite_Msg(ulong param_1, ushort * ...
void                  <VOID>        <RETURN>
ulong                 ECX:4         param_1
ushort *              RDX:8         param_2
ulong                 R8D:4         param_3
char *                R9:8          param_4
                    ?TEventWrite_Msg@@YAXKPEBGKPEAG@Z              XREF[451]:   FUN_7ff76f0101
                    ?Notify@?$TConsumer@VTIniSpoolerWrapper@@@NThr...           FUN_7ff76f0111
                    ?OutsidePackageLock@NPackageInstallLocalspl@@Y...           SplOpenPrinter
                    ?Print@TANAttributes@NAsyncNotifyLocalspl@@QEA...           CreateServerHa
                    ??1TErrorHandler@NDPS_UtilityLibrary@@QEAA@XZ               CreateServerHa
                    ?TEventWrite_Msg@@YAXKPEBGKPEAD@Z                           SplOpenPrinter
```

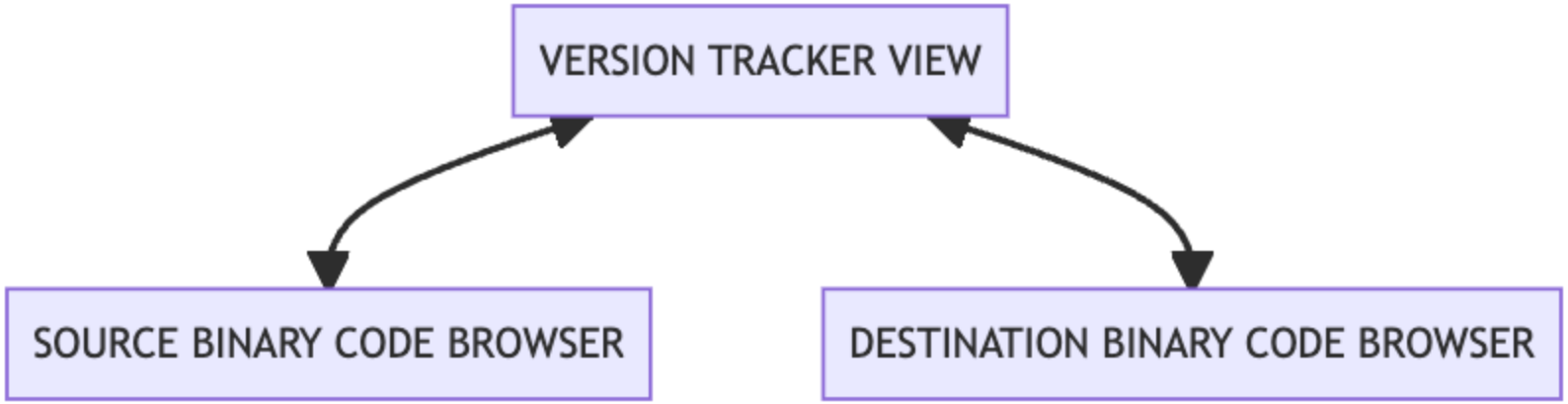
Destination: **TEventWrite_Msg()** in /2020-05/p..ooler-core-localspl_6.1.7601.24554/localspl.dll

```
                    **************************************************************
                    * void __cdecl TEventWrite_Msg(unsigned long,unsigned sho... *
                    **************************************************************
                    void __fastcall TEventWrite_Msg(ulong param_1, ushort * ...
void                  <VOID>        <RETURN>
ulong                 ECX:4         param_1
ushort *              RDX:8         param_2
ulong                 R8D:4         param_3
char *                R9:8          param_4
                    ?TEventWrite_Msg@@YAXKPEBGKPEAG@Z              XREF[451]:   FUN_7ff76f0101
                    ?Notify@?$TConsumer@VTIniSpoolerWrapper@@@NThr...           FUN_7ff76f0111
                    ?OutsidePackageLock@NPackageInstallLocalspl@@Y...           SplOpenPrinter
                    ?Print@TANAttributes@NAsyncNotifyLocalspl@@QEA...           CreateServerHa
                    ??1TErrorHandler@NDPS_UtilityLibrary@@QEAA@XZ               CreateServerHa
                    ?TEventWrite_Msg@@YAXKPEBGKPEAD@Z                           SplOpenPrinter
```

Auto Version Tracking Command completed successfully with no apply markup errors.

Analyst View

The workflow is performed within the Version Tracker Tool GUI which opens several windows (Ghidra loves its windows). The following windows will open once initial setup is complete.



Ghidra Patch Diffing

Version Tracking (SOURCE TOOL): WindowsPrintSpooler:/2020-04/p..ooler-core-localspl_6.1.7601.24383/localspl.dll

File Edit Analysis Graph Navigation Search Select Tools Window Help

Program Trees

- localspl.dll
  - Headers
  - .text
  - .rdata
  - .data
  - .pdata
  - .rsrc
  - .reloc
  - Debug Data

Program Tree

Data Type Manager

- Data Types
  - BuiltInTypes
  - localspl.dll
  - winapi_64
  - windows_vs12_64

Filter:

Listing: localspl.dll

```
                    undefined4          Stack[0x10]:4  local_res10

                    undefined8          Stack[0x8]:8   local_res8

                    undefined8          Stack[-0x38]:8 local_38

                                  ?GetPrinterSize@@YAKPEAU_INIPRINT
                                  GetPrinterSize
7ff76f0159c 48 89 5c        MOV        qword ptr [RSP +
            24 08
7ff76f015a1 48 89 6c        MOV        qword ptr [RSP +
            24 18
7ff76f015a6 48 89 74        MOV        qword ptr [RSP +
            24 20
7ff76f015ab 57              PUSH       RDI
7ff76f015ac 41 54           PUSH       R12
7ff76f015ae 41 55           PUSH       R13
7ff76f015b0 41 56           PUSH       R14
7ff76f015b2 41 57           PUSH       R15
7ff76f015b4 48 83 ec 30     SUB        RSP,0x30
7ff76f015b8 33 db           XOR        EBX,EBX
7ff76f015ba 4d 8b e9        MOV        R13,param_4
7ff76f015bd 4c 8b e1        MOV        R12,param_1
7ff76f015c0 8d 6b 01        LEA        EBP,[RBX + 0x1]
7ff76f015c3 3b d3           CMP        param_2,EBX
7ff76f015c5 0f 84 b8        JZ         LAB_7ff76f1fb83
            e5 01 00
7ff76f015cb 2b d5           SUB        param_2,EBP
7ff76f015cd 0f 84 6c        JZ         LAB_7ff76f1c63f
```

Decompile: GetPrinter...

```
/* unsigned long __cdecl GetPrinterSize
   long,unsigned short * __ptr64,struct

uint GetPrinterSize(longlong param_1,in

{
  short sVar1;
  DWORD DVar2;
  int iVar3;
  longlong lVar4;
  int iVar5;
  uint uVar6;
  int iVar7;
  short *psVar8;
  int iVar9;
  int iVar10;
```

Version Tracking Matches for Source

Source Label: GetPrinterSize Label Type: Analysis Source

1	...	...	...	...	D...	Des...	2	...	...	Alg...
	...	...	2	0	Gl...	Get...	7...	...	...	Ex...
	...	...	2	0	Gl...	Get...	7...	...	...	Ex...
	...	...	2	0	Gl...	Get...	7...	...	...	Co...
	...	...	2	0	Gl...	Get...	7...	...	...	Ex...

7ff76f0159c GetPrinterSize MOV qword ptr [RSP + 0x8],RBX

Version Tracking (DESTINATION TOOL): WindowsPrintSpooler:/2020-05/p..ooler-core-localspl_6.1.7601.24554/localspl.dll

File Edit Analysis Graph Navigation Search Select Tools Window Help

Program Trees

- localspl.dll
  - Headers
  - .text
  - .rdata
  - .data

Program Tree

Data Type Manager

- Data Types
  - BuiltInTypes
  - localspl.dll
  - spooler_types
  - winapi_64
  - windows_vs12_64

Filter:

Listing: loc...

```
                    undefined8          Sta

                    undefined8          Sta

                                  ?GetP
                                  GetPr
7ff76f0159c 48 89 5c        M
            24 08
7ff76f015a1 48 89 6c        M
            24 18
7ff76f015a6 48 89 74        M
            24 20
7ff76f015ab 57              P
7ff76f015ac 41 54           P
7ff76f015ae 41 55           P
7ff76f015b0 41 56           P
7ff76f015b2 41 57           P
```

Decompile: GetPrinterSize - (localspl.dll)

```
/* unsigned long __cdecl GetPrinterSize(struct _INIPRINTER * __ptr64,u
   long,unsigned short * __ptr64,struct _devicemodeW * __ptr64) */

uint GetPrinterSize(longlong param_1,int param_2,undefined8 param_3,sh

{
  short sVar1;
  DWORD DVar2;
  int iVar3;
  longlong lVar4;
  int iVar5;
  uint uVar6;
  int iVar7;
  short *psVar8;
  int iVar9;
  int iVar10;
  int iVar11;
  int iVar12;
```

Version Tracking Matches for Destination

Destination Label: GetPrinterSize Label Type: Analysis Destination Address: 7ff76f0159c

Function Call Trees: GetPrinterSize - (localspl.dll)

Incoming Calls

- Incoming References - GetPrinterSize
  - SplEnumPrinters
  - SplGetPrinter

Outgoing Calls

- Outgoing References - GetPrinterSize
  - GetSecurityDescriptorLength
  - GetPrinterPorts

Filter:

7ff76f0159c GetPrinterSize MOV qword ptr [RSP + 0x8],RBX

Maddie Stone
@maddiestone

Thanks for all your suggestions. Based on this, I tested:
DarunGrim
BinDiff
Diaphora
radiff2
(I forgot Ghidra 🤢 but will update with that)

For the scoped problem of patch diffing for CVE-2019-3568, BinDiff was the only one that performed successfully.

github.com/maddiestone/Co...

> **Maddie Stone** @maddiestone · Aug 13, 2019
> What are your favorite binary diffing/ patch diffing tools and why? It's been a few years so I'd like to know what are the new releases and/or what are the old stand-bys that continue to perform? RTs appreciated

4:06 PM · Oct 11, 2019

Version Tracking Tool

- Some insightful match function algorithms
- Missing well-known function matching algorithms
- Lacks a pseudo code diff view
- Confusing Similarity Scoring
- A bit slow
- Will get you there eventually

Binary Diffing Tools - Workflow

Standard Binary Diffing Workflow

1. Obtain two binaries to diff (old and new)
2. Create new SRE project
3. Import old and new binary
4. Run analysis on binaries
5. Run diffing heuristics
6. Export the analysis for each file
7. Open up the exported analysis in the corresponding diff tool
8. Analyze the diff

Modern Windows Patch Diffing Workflow

Security Update Guide

The Microsoft Security Response Center (MSRC) investigates all reports of security vulnerabilities affecting Microsoft products and services, and provides the information here as part of the ongoing effort to help you manage security risks and help keep your systems protected.

All Deployments **Vulnerabilities**

Select date range Edit columns Download Filters

kernel No grouping Clear

Release date	Last Updat...	CVE Number ↓	CVE Title	Impact	Max Severity	Tag
Sep 12, 2023	-	CVE-2023-38150	Windows Kernel Elevation of Priv	Elevation of Privile	Important	Windows Kernel
Sep 12, 2023	-	CVE-2023-38142	Windows Kernel Elevation of Priv	Elevation of Privile	Important	Windows Kernel
Sep 12, 2023	-	CVE-2023-38141	Windows Kernel Elevation of Priv	Elevation of Privile	Important	Windows Kernel
Sep 12, 2023	-	CVE-2023-38140	Windows Kernel Information Dis	Information Discl	Important	Windows Kernel
Sep 12, 2023	-	CVE-2023-38139	Windows Kernel Elevation of Priv	Elevation of Privile	Important	Windows Kernel
Sep 12, 2023	-	CVE-2023-36803	Windows Kernel Information Dis	Information Discl	Important	Windows Kernel

Release ... ↓	Product	Impact	Max Severity	Article	Download	Build Number
Sep 12, 2023	Windows 11 Version 22H2 for x64-based Systems	Elevation of Privilege	Important	5030219	Security Update	10.0.22621.2283
Sep 12, 2023	Windows 11 Version 22H2 for ARM64-based Systems	Elevation of Privilege	Important	5030219	Security Update	10.0.22621.2283
Sep 12, 2023	Windows 11 version 21H2 for ARM64-based Systems	Elevation of Privilege	Important	5030217	Security Update	10.0.22000.2416
Sep 12, 2023	Windows 11 version 21H2 for x64-based Systems	Elevation of Privilege	Important	5030217	Security Update	10.0.22000.2416

ntoskrnl.exe - Winbindex

NT Kernel & System

Show 10 entries

Search:

SHA256	Windows	Update	File arch	File version	File size	Extra	Download
ae09a8...	Windows 11 22H2	KB5030310	x64	10.0.22621.2361	11.53 MB	Show	Download
9e0a3a...	Windows 11 21H2	KB5030301	x64	???	11.21 MB	Show	Download
2ee300...	Windows 10 22H2	KB5030300	x64	10.0.19041.3516	10.37 MB	Show	Download
1ed128...	Windows 10 1507	KB5030220	x64	10.0.10240.20161	7.66 MB	Show	Download
d67c38...	Windows 11 22H2	KB5030219	x64	10.0.22621.2283	11.54 MB	Show	Download
0a1ff4...	Windows 11 21H2	KB5030217	x64	10.0.22000.2416	11.21 MB	Show	Download
64de05...	Windows 10 1809	KB5030214	x64	10.0.17763.4851	9.23 MB	Show	Download
310c55...	Windows 10 1607	KB5030213	x64	10.0.14393.6252	7.43 MB	Show	Download
d436d6...	Windows 10 21H2 (+1)	KB5030211	x64	10.0.19041.3448	10.37 MB	Show	Download
9f0ad4...	Windows 11 22H2	KB5029351	x64	10.0.22621.2215	11.54 MB	Show	Download
SHA256	**Windows**	**Update**	**File arch**	**File version**	**File size**	**Extra**	**Download**

Showing 1 to 10 of 742 entries

Previous 1 2 3 4 5 ... 75 Next

File Edit Project Tools Help Ghidra: ntoskernl-test-cnre...

Tool Chest

Active Project: ntoskernl-test-cnrename

- ntoskernl-test-cnrename
  - ntkrnlmp.exe.x64.10.0.22621.1344
  - ntkrnlmp.exe.x64.10.0.22621.1413
  - s1
  - s2

Filter:

Tree View Table View

Running Tools

Workspace

Opened project: ntoskernl-test-cnrename

File Edit Window Help

Version Tracking: s2

Version Tracking Matches - [Session: s2] - 36997 matches (of 55281)

Tag	Session...	Status	Type	Score	Confid...	Votes	# Confli...	Multipl...	Source Na...	Source Label	Source ...	Multiple ...	Dest Na...	Dest Label	Dest Ad...	Source...	Dest Le...	Algorithm
	1		Function	1.000	1.000	0	0	2	SC_DISK	~SC_DISK	140661...	2	SC_DISK	~SC_DI...	140661...	237	237	Exact Symbol ...
	1		Function	1.000	1.000	0	0	2	SC_DEVICE	~SC_DEVICE	140662...	2	SC_DEVI...	~SC_D...	140662...	183	183	Exact Symbol ...
	1		Function	1.000	1.000	0	0	2	Global	ZwYieldExecution	140425...	2	Global	ZwYiel...	140425f...	30	30	Exact Symbol ...
	1		Function	1.000	1.000	0	0		Global	ZwWriteVirtualMem...	140425...		Global	ZwWri...	140425...	30	30	Exact Symbol ...
	1		Function	1.000	1.000	0	0	2	Global	ZwWriteFile	140425...	2	Global	ZwWri...	140425...	30	30	Exact Symbol ...
	1		Function	1.000	1.000	0	0	2	Global	ZwWaitForSingleObj...	140425...	2	Global	ZwWai...	140425...	30	30	Exact Symbol ...

Filter: | Score Filter: 0.000 to 1.000 | Confidence Filter: -9.999 to 9.999 | Length Filter: 0

Version Tracking Functions - [Session: s2] - Source Functions - 4041 functions (of 32775) / Destination Functions - 4042 functions (of 32776)

Source = ntoskernl-test-cnrename:/ntkrnlmp.exe.x64.10.0.22621.1344

Label	Location	Function Signature	Function Size
FUN_140b07730	140b07730	undefined FUN_...	108830

Filter:

Destination = ntoskernl-test-cnrename:/ntkrnlmp.exe.x64.10.0.22621.1413

Label	Location	Function Signature	Function Size
FUN_140b07730	140b07730	undefined FUN_1...	108830

Filter:

Decompile View | Listing View

Source: **FUN_140b07730()** in /ntkrnlmp.exe.x64.10.0.22621.1344

```
                    ****************************************
                    *                FUNCTION              *
                    ****************************************
                    undefined FUN_140b07730(undefined pa...
                      assume GS_OFFSET = 0xff000...
          undefined   AL:1       <RETURN>
          undefined   CL:1       param_1
```

Destination: **FUN_140b07730()** in /ntkrnlmp.exe.x64.10.0.22621.1413

```
                    ****************************************
                    *                FUNCTION              *
                    ****************************************
                    undefined FUN_140b07730(undefined pa...
                      assume GS_OFFSET = 0xff000...
          undefined   AL:1       <RETURN>
          undefined   CL:1       param_1
```

Version Tracking Marku... × | Version Tracking Impli... × | Version Tracking Funct... ×

Export ntkrnlmp.exe.x64.10.0.22621.1344

Format: Binary BinExport (v2) for BinDiff

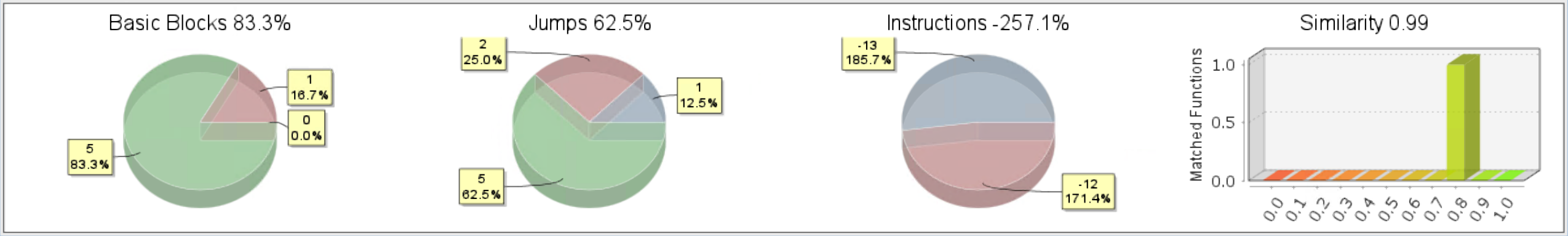
Output File: C:\Users\user\Desktop\ntkrnlmp.exe.x64.10.0.22621.1344

Export ntkrnlmp.exe.x64.10.0.22621....

Exporting meta data

Cancel

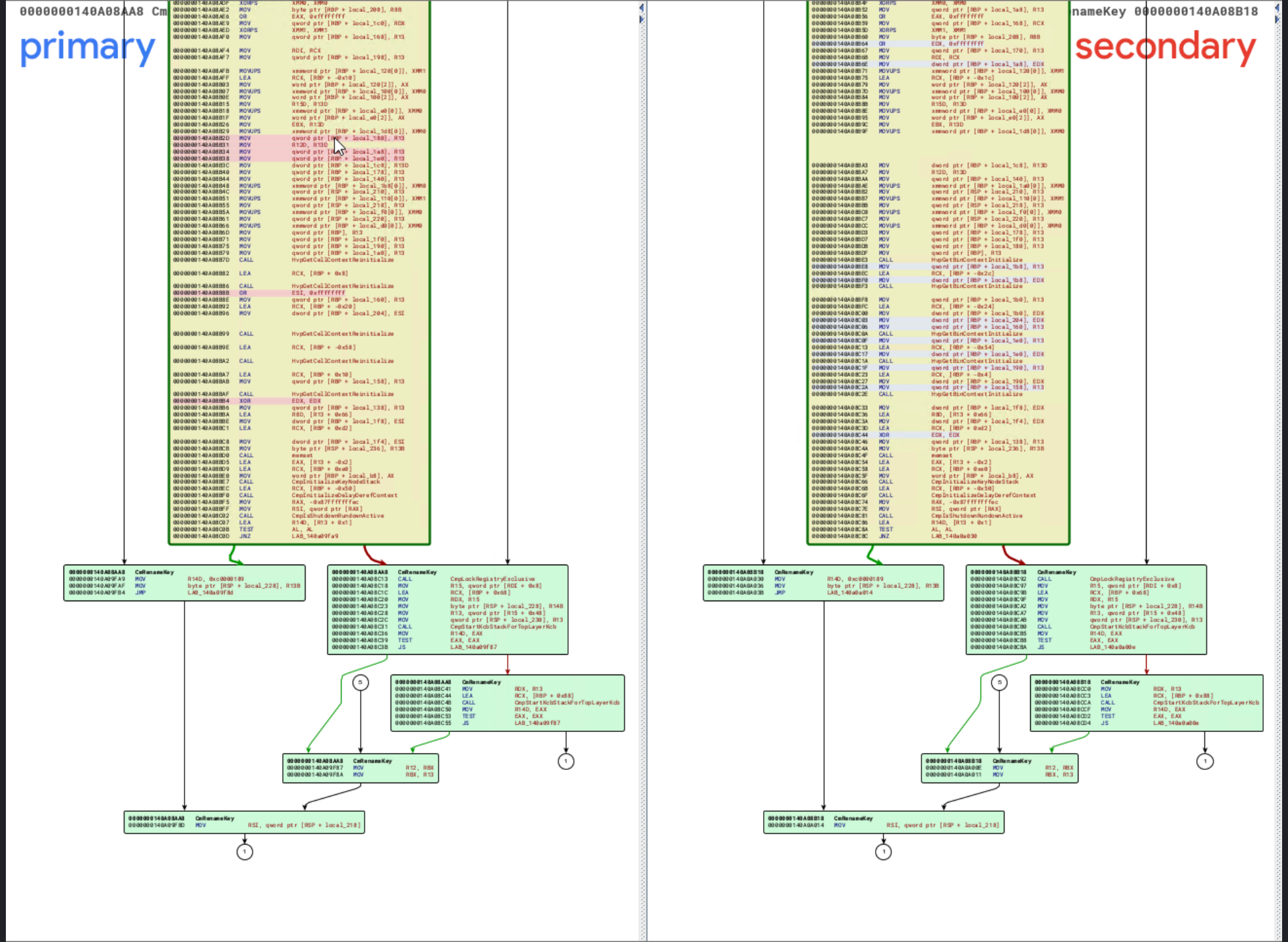
Overview



32856 / 32856 Matched Functions

☑ Show structural changes ☑ Show only instructions changed ☑ Show identical

Similarity	Confidence	Address	Primary Name	Type	Address	Secondary Name	Type	Basic Blocks	Jumps
0.33	0.50	000000...	NtTranslateFilePath$filt$0	Normal	000000...	NtTranslateFilePath$filt$0	Normal	1 1 0	
0.38	0.73	000000...	ExpKdPullRemoteFileForU...	Normal	000000...	ExpKdPullRemoteFileForU...	Normal	0 1 2	2
0.42	0.73	000000...	KiVerifyXcpt10fin1	Normal	000000...	KiVerifyXcpt10fin1	Normal	0 1 1	1
0.42	0.73	000000...	NtEnumerateBootEntries$...	Normal	000000...	NtEnumerateBootEntries$...	Normal	1 1 0	1
0.44	0.73	000000...	CmQueryFeatureConfigurat...	Normal	000000...	CmQueryFeatureConfigurat...	Normal	1 1 0	1
0.75	0.99	000000...	SPCallServerHandleClepKdf	Normal	000000...	SPCallServerHandleClepKdf	Normal	11 12 0	20 20 0
0.83	0.99	000000...	MiPreserveBootDecisions	Normal	000000...	MiPreserveBootDecisions	Normal	10 30 0	23 41 6
0.85	0.95	000000...	HalpMiscGetParameters	Normal	000000...	HalpMiscGetParameters	Normal	2 66 10	16 92 30
0.87	**0.99**	**000000...**	**KiVerifyXcpt2fin0**	**Normal**	**000000...**	**KiVerifyXcpt2fin0**	**Normal**	**1 5 0**	**2 5 1**
0.89	0.99	000000...	KeQuerySpeculationContro...	Normal	000000...	KeQuerySpeculationContro...	Normal	0 33 11	3 48 20
0.89	0.97	000000...	WritePartitionTable	Normal	000000...	WritePartitionTable	Normal	4 59 3	24 74 25
0.96	0.99	000000...	KiDetectHardwareSpecCon...	Normal	000000...	KiDetectHardwareSpecCon...	Normal	0 80 3	8 117 12
0.99	0.99	000000...	CmRenameKey	Normal	000000...	CmRenameKey	Normal	0 292 1	7 481 8
0.99	0.99	000000...	Phase1InitializationDiscard	Normal	000000...	Phase1InitializationDiscard	Normal	1 213 0	2 336 1
1.00	0.99	000000...	HvlQueryActiveHypervisor...	Normal	000000...	HvlQueryActiveHypervisor...	Normal	0 3 0	0 2 0
1.00	0.99	000000...	CmpTraceHiveSaveStop	Normal	000000...	CmpTraceHiveSaveStop	Normal	0 3 0	0 4 0
1.00	0.99	000000...	IoIsActivityTracingEnabled	Normal	000000...	IoIsActivityTracingEnabled	Normal	0 4 0	0 4 0


0000000140A08AA8 CmRenameKey
primary
nameKey 0000000140A08B18
secondary

Binary Diffing Tools - Under the Hood


GHIDRIFF
GHIDRA

Standing on the Shoulders of Giants

- BinDiff - IDA / Ghidra / BinaryNinja
- Diaphora - IDA
- Version Tracking - Ghidra
- Ghidriff - Ghidra

Function Matching

- Binary diffing is just a game of matching functions
- Each tool attempts to match all recognized functions
- Start with fast and accurate, progress to slow and speculative

BinDiff - algorithms

Function Matching

Function attributes are used in one of two ways. Either canonically per function or per edge. Edge matching tries to match edges (which represent calls in the call graph or jumps in the flow graphs) if source and target function attributes match. Thus edge matching is the stronger criterium, yielding better matches in general. However, since it is possible to have a lot of edges per vertex in a graph (this is especially true for callgraphs, where the number of edges often grows super linearily in the number of vertices) edge matching may potentially be very slow. If you do encounter performance problems for certain binaries you should first try to disable edge matching based algorithms. Also, do not hesitate to send the offending binaries to the zynamics team at Google - we are always trying to improve performance bottlenecks and are grateful for samples.

Function matching algorithms ordered roughly by resulting match quality:

function: hash matching

> Matches functions based on a hash of the original raw function bytes. Thus two functions matched by this algorithm should be identical on the byte level.
>
> match quality: very good
>
> algorithm performance: very good

function: name hash matching

> Matches functions based on a hash of their names. Only *real* names are considered, names which have been auto-generated by the disassembler are not used. This is one of the few algorithms that can match imported functions, i.e. functions that do not have an actual body in the binary. False matches are highly unlikely.
>
> match quality: very good
>
> algorithm performance: very good

function: edges flowgraph MD index

> Matches callgraph edges based on their source and target function's MD indices. Thus calls between two structurally identical functions are matched.
>
> match quality: very good
>
> algorithm performance: medium

function: edges callgraph MD index

> Matches callgraph edges based on their callgraph MD index. This means the callgraph leading to that particular call is structurally identical in both binaries. Match quality depends on how deep the callstack leading up to this edge is: the deeper the less likely is a false match.
>
> match quality: good
>
> algorithm performance: medium

function: MD index matching (flowgraph MD index, top down), function: MD index matching (flowgraph MD index, bottom up)

> Matches functions based on their structure using the MD index. Since the MD index takes a topological graph ordering as one of it's inputs we can parametrize it by whether we sort the graph vertices into levels following calls from the entrypoint (top down) or callers from the exit points (bottom up).
>
> match quality: good

Diaphora - heuristics

Diaphora Heuristics

Heuristics implemented in Diaphora and how to add new ones

Diaphora Heuristics

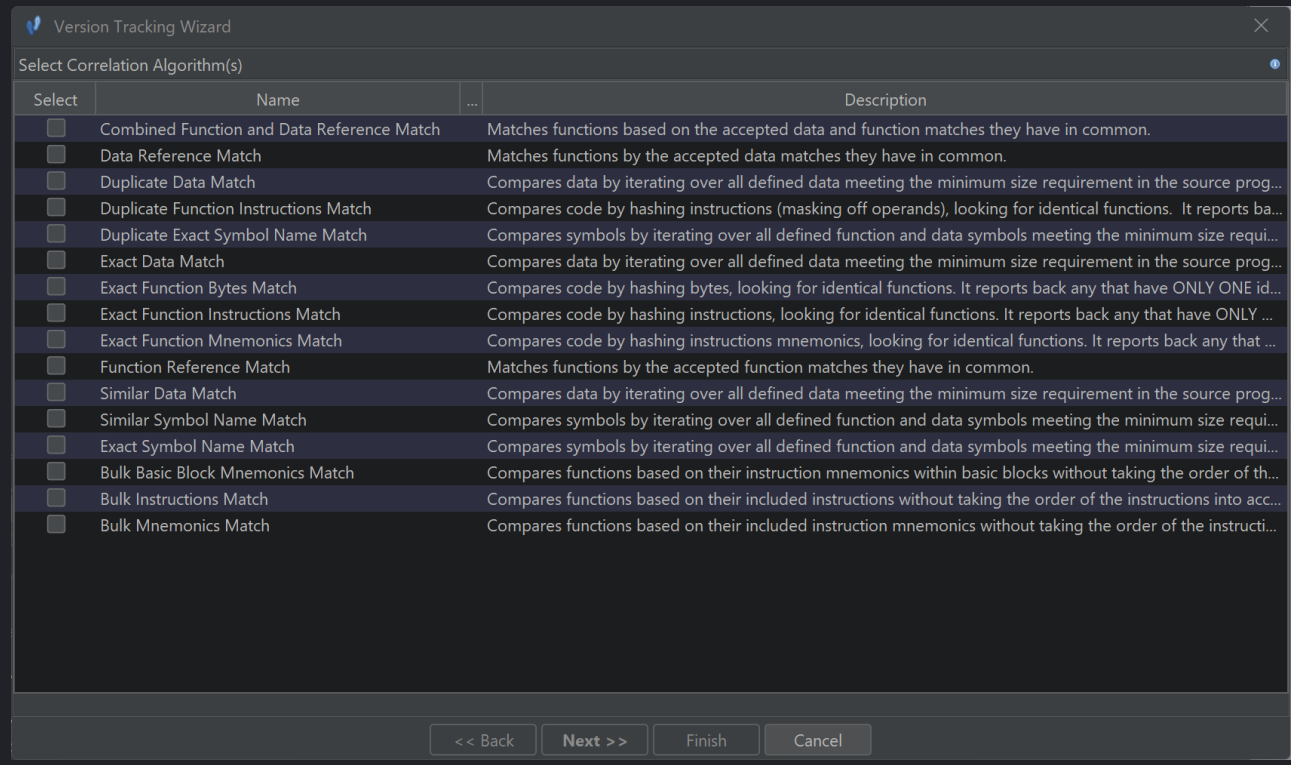
Diaphora uses multiple heuristics to find matches between different functions. The next list shows all the heuristics implemented in the current Diaphora Release.

Best matches

The very first thing Diaphora tries is to find if everything in both databases, even the primary key values are equals. If so, the databases are considered 100% equals and nothing else is done. After that, it runs a number of heuristics for which the results are known to be very good and realible.

- **Equal pseudo-code**. The pseudo-code generated by the Hex-Rays decompiler are equals. It can match code from x86, x86_64 and ARM interchangeably.
- **Equal assembly**. The assembly of both functions is exactly equal.
- **Bytes hash and names**. The first byte of each assembly instruction is equal and also the referenced true names, not IDA's auto-generated ones, have the same names.
- **Same address, nodes, edges and mnemonics**. The number of basic blocks, their addresses, the names of edges and the mnemonics in both databases are equal.
- **Same RVA and hash**. The RVA (Relative Virtual Address) and the bytes hash is the same for both databases.
- **Same order and hash**. Both functions have the same bytes hash and were discovered by IDA at the very same position in the database (i.e., both functions are the 100th function in the database).
- **Function hash**. The calculated function hash is equal for both functions. The hash is calculated as the MD5 of the concatenation of all the instruction bytes in a function.
- **Bytes hash**. The calculated bytes hash is equal for both functions. The hash is calculated as the MD5 of the concatenation of all the instruction bytes in a function but, in opposite to function hash, it does so by stripping any byte that can be variable depending on the address of the instruction, like displacements or relative calls and jumps.
- **Bytes sum**. Both the size of the function in bytes and the summatory of all the bytes in the function are the same for both functions.

Ghidra - correlators



3 General Matching Methods

- **Syntax** - compare representation of actual bytes or sequence of instructions
- **Semantics** - compare the meaning is equivalent or provide the same functionality
- **Structure** - a blend of semantic and syntax; analyzes graph representations of binaries (control flow, callgraphs, etc.) and computes similarity on these generated structures

Syntax Matching - Exact Bytes Hash

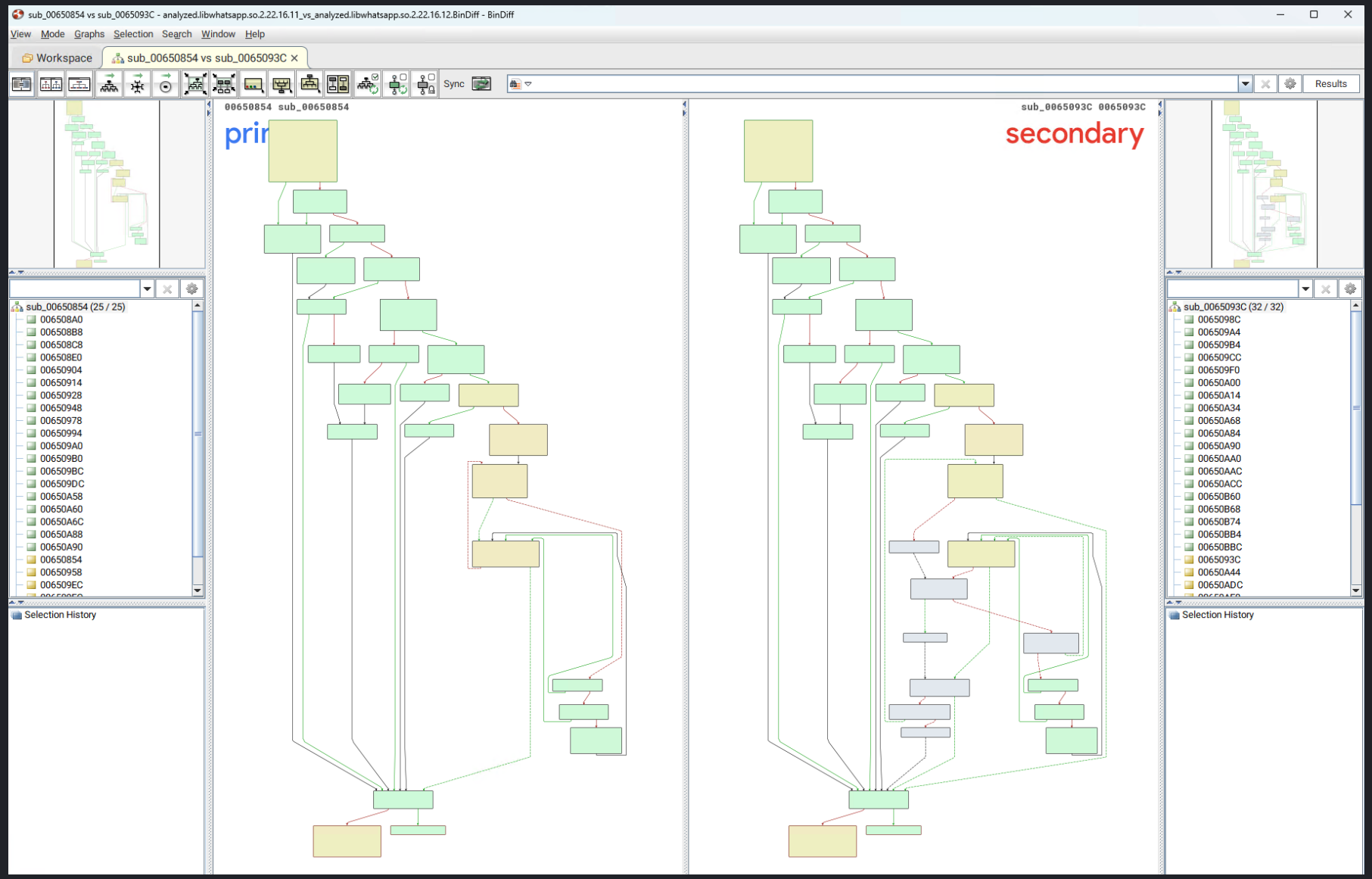
```
29    public class ExactBytesFunctionHasher extends AbstractFunctionHasher {
44            protected long hash(TaskMonitor monitor, ArrayList<CodeUnit> units, int byteCount)
48                    for (CodeUnit codeUnit : units) {
49                            monitor.checkCancelled();
50
51                            try {
52                                    codeUnit.getBytesInCodeUnit(buffer, offset);
53                            }
54                            catch (MemoryAccessException e) {
55                                    Msg.warn(this, "Could not get code unit bytes at " + codeUnit.getAddress());
56                            }
57                            offset += codeUnit.getLength();
58                    }
59                    if (offset != byteCount) {
60                            throw new IllegalStateException("did NOT use all the codeUnit buffer bytes");
61                    }
62                    synchronized (digest) {
63                            digest.reset();
64                            digest.update(buffer, monitor);
65                            return digest.digestLong();
66                    }
```

Structural Matching

> A relatively simple [...] heuristic for telling whether two graphs are isomorphic is to compare the number of nodes and edges.

Halvar Flake 2004

Structural Comparison of Executable Objects


sub_00650854 vs sub_0065093C - analyzed.libwhatsapp.so.2.22.16.11_vs_analyzed.libwhatsapp.so.2.22.16.12.BinDiff - BinDiff
View Mode Graphs Selection Search Window Help
Workspace
sub_00650854 vs sub_0065093C
Sync
Results
00650854 sub_00650854
prir
sub_0065093C 0065093C
secondary
sub_00650854 (25 / 25)
006508A0
006508B8
006508C8
006508E0
00650904
00650914
00650928
00650948
00650978
00650994
006509A0
006509B0
006509BC
006509DC
00650A58
00650A60
00650A6C
00650A88
00650A90
00650854
00650958
006509EC
Selection History
sub_0065093C (32 / 32)
0065098C
006509A4
006509B4
006509CC
006509F0
00650A00
00650A14
00650A34
00650A68
00650A84
00650A90
00650AA0
00650AAC
00650ACC
00650B60
00650B68
00650B74
00650BB4
00650BBC
0065093C
00650A44
00650ADC
Selection History

All tools look to provide the complete list of matches

Function Classification

Classification	old binary	new binary
Deleted	Unmatched	X
Added	X	Unmatched
Modified	Matched but different	Matched but different

With the full diff you can start to make sense of the changes

- Deleted
  - KERNEL32.DLL::DeleteFileW
- Added
  - StringCchCatW
  - WPP_SF_SD
  - AllocAndCatString
  - ConvertFullPathToLongUNC
  - IsValidFilePath
  - SafeDeleteFileByHandle
  - WPP_SF_SS
  - KERNEL32.DLL::SetFileInformationByHandle
  - KERNEL32.DLL::GetFinalPathNameByHandleW
  - MSVCRT.DLL::_wcsnicmp
  - MSVCRT.DLL::wcsnlen
  - KERNEL32.DLL::GetFileInformationByHandle
- Modified
  - CDeviceRoutingInfo::ConfigChange
  - FaxRouteGetRoutingInfo
  - IsValidFaxFolder
  - WPP_SF_S
  - FaxRouteSetRoutingInfo

Sometimes new functions are **added** to address security issues:

- Added
  - StringCchCatW
  - WPP_SF_SD
  - AllocAndCatString
  - ConvertFullPathToLongUNC
  - IsValidFilePath
  - SafeDeleteFileByHandle
  - WPP_SF_SS
  - KERNEL32.DLL::SetFileInformationByHandle
  - KERNEL32.DLL::GetFinalPathNameByHandleW
  - MSVCRT.DLL::_wcsnicmp
  - MSVCRT.DLL::wcsnlen
  - KERNEL32.DLL::GetFileInformationByHandle

Previously vulnerable functions will be **deleted** and the functions using them **modified** to use the new safer APIs

```
-       BVar3 = DeleteFileW(local_238);
-       if (BVar3 == 0) {
+       iVar4 = SafeDeleteFileByHandle((ushort *)local_238);
+       if (iVar4 == 0) {
          DVar1 = GetLastError();
          if ((((undefined **)WPP_GLOBAL_Control != &WPP_GLOBAL_Control) &&
              ((WPP_GLOBAL_Control[0x1c] & 2) != 0)) && (1 < (byte)WPP_GLOBAL_Contro
-           uVar4 = 0x57;
+           uVar5 = 0x5c;
            goto LAB_1;
          }
        }
      }
    }
```

Patch diffing will not tell you *which* functions are relevant

Patch diffing will help you focus solely on the functions that could be

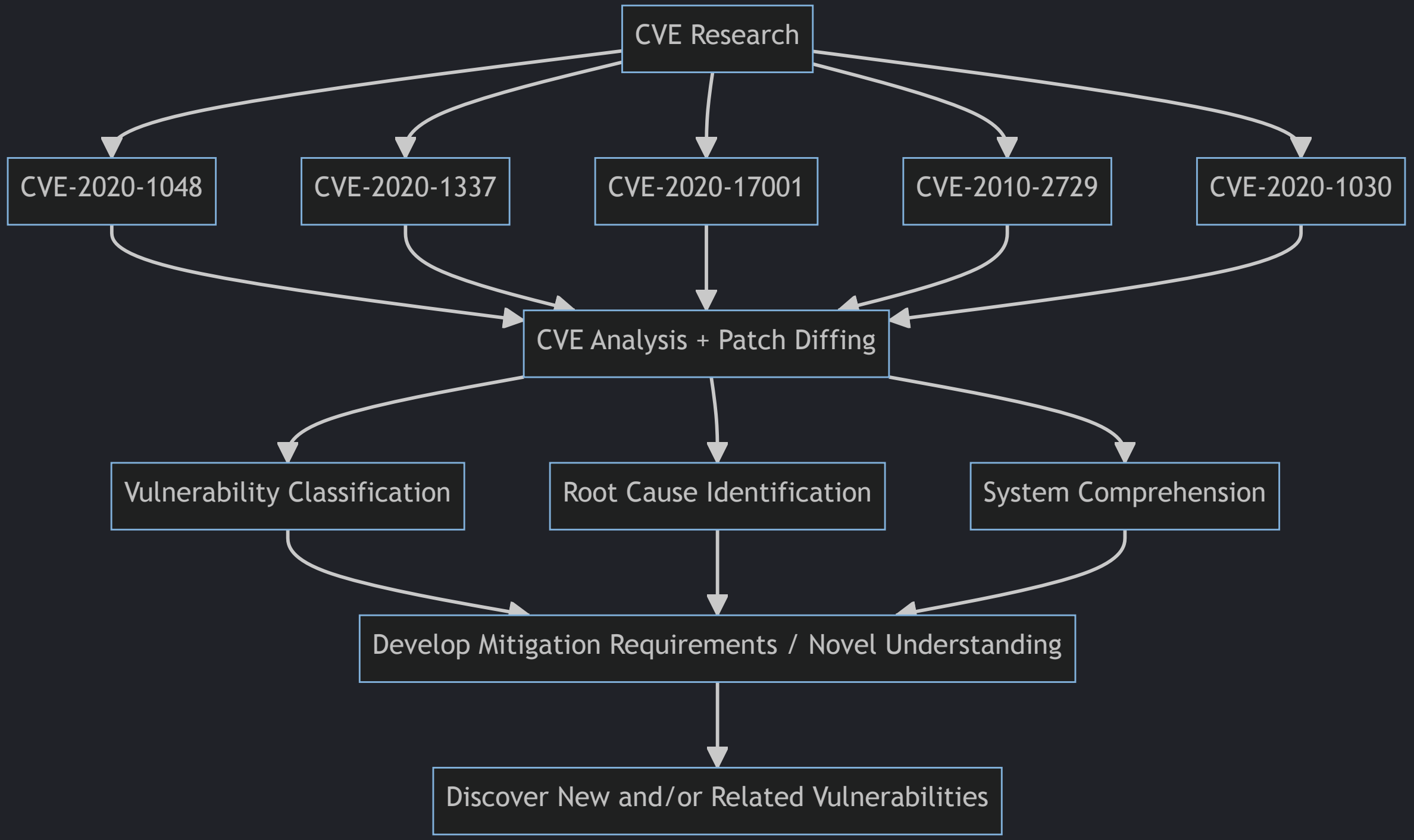
Background / Motivation

CVE North Stars

Leveraging CVEs as North Stars in vulnerability discovery and comprehension.

Created: 2020-12-15 Updated: 2023-09-27

Get started View on GitHub


CVE Research
CVE-2020-1048
CVE-2020-1337
CVE-2020-17001
CVE-2010-2729
CVE-2020-1030
CVE Analysis + Patch Diffing
Vulnerability Classification
Root Cause Identification
System Comprehension
Develop Mitigation Requirements / Novel Understanding
Discover New and/or Related Vulnerabilities

"It is often used to determine the technical details behind ambiguously-worded bulletins, and to establish the root causes, attack vectors and potential variants of the vulnerabilities in question."

using-binary-diffing-to-discover

Project Zero

News and updates from the Project Zero team at Google

Thursday, October 5, 2017

Using Binary Diffing to Discover Windows Kernel Memory Disclosure Bugs

Posted by Mateusz Jurczyk of Google Project Zero

Patch diffing is a common technique of comparing two binary builds of the same code – a known-vulnerable one and one containing a security fix. It is often used to determine the technical details behind ambiguously-worded bulletins, and to establish the root causes, attack vectors and potential variants of the vulnerabilities in question. The approach has attracted plenty of research [1][2][3] and tooling development [4][5][6] over the years, and has been shown to be useful for identifying so-called 1-day bugs, which can be exploited against users who are slow to adopt latest security patches. Overall, the risk of post-patch vulnerability exploitation is inevitable for software which can be freely reverse-engineered, and is thus accepted as a natural part of the ecosystem.

Labs

HOME VULN. DISCLOSURE POLICY CONTACT

BY ALIZ HAMMOND — JUN 13, 2023

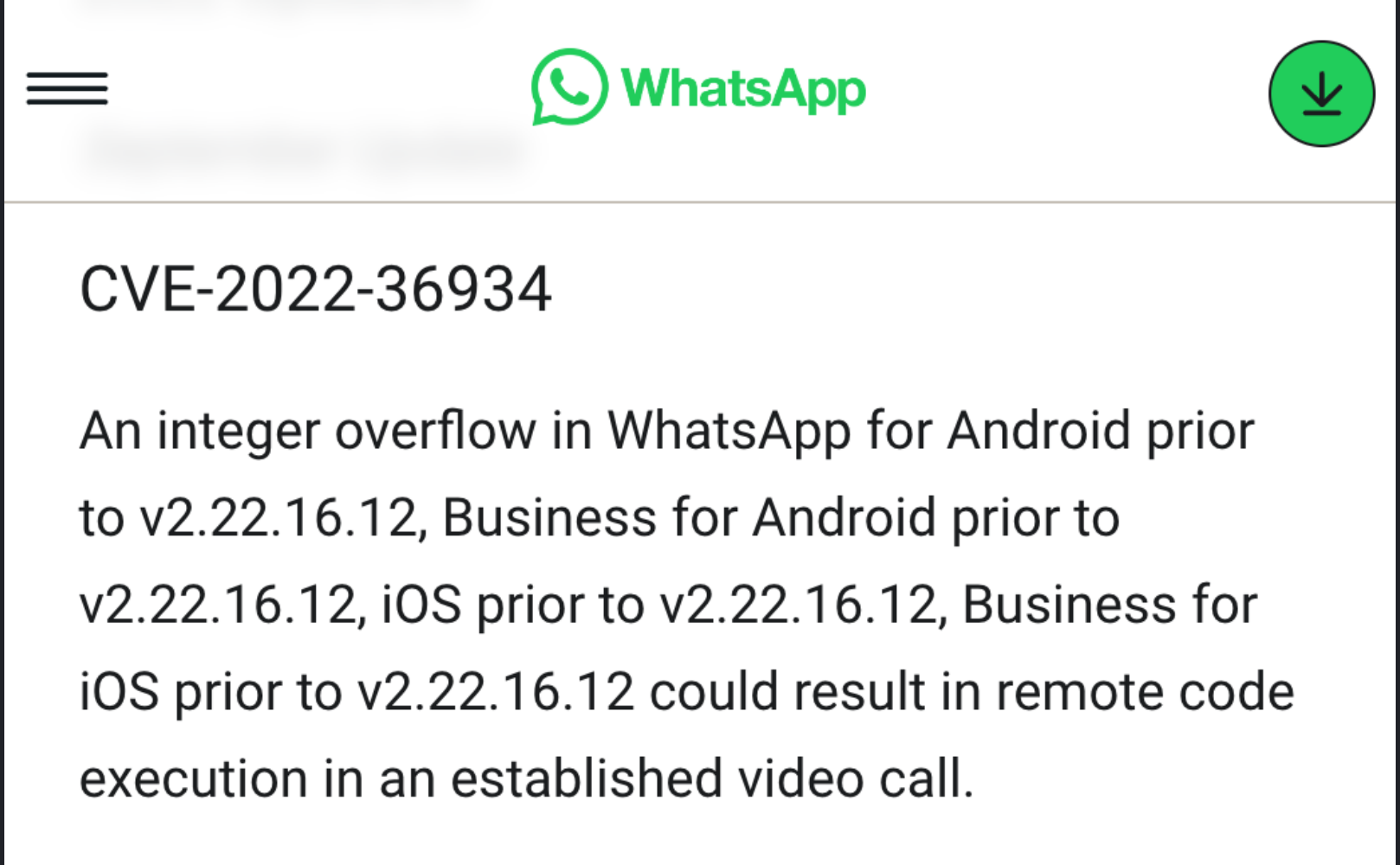
Xortigate, or CVE-2023-27997 - The Rumoured RCE That Was

(Sorry for using the same meme again, but we love it)

"Since fixes for the vulnerable devices were quietly published by Fortinet, we decided to dive in and 'patch diff' the bug, [...]to locate details of the fix..."

xortigate-or-cve-2023-27997

Patch Diffing in the Dark



Patch Diffing

“

- is a single source of truth when there is no other
- provides clarity in root cause analysis
- can improve your competence in reverse engineering and understanding of modern vulnerabilities

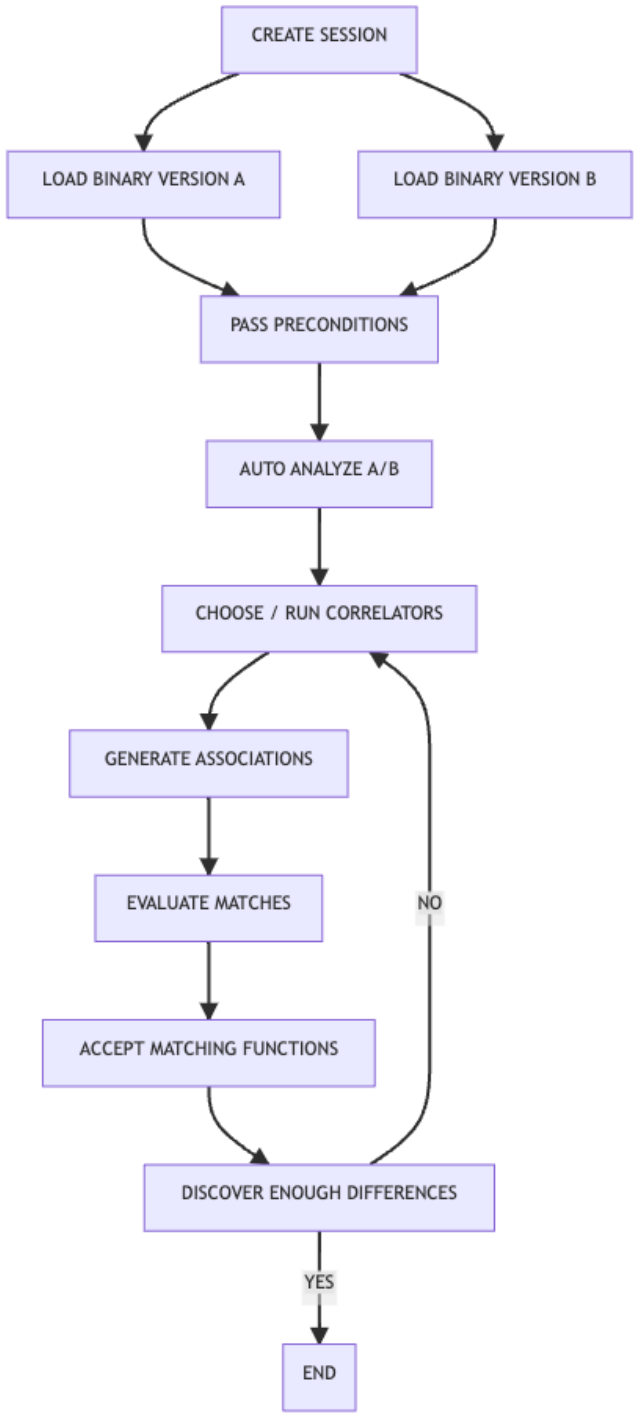
”

CVE North Stars

Patch diffing became a permanent tool in my RE tool belt

Patch Diffing All Day Every Day

- Useful to dive deep in a new area of research
- Fun friday night scoped RE practice
- Started to get good at the VT Workflow



It became repetitive and tedious...

What do programmers do when they encounter a repetitive tedious task?

ghidriff

Private

Unwatch 3

generated from clearbluejar/ghidra-python-vscode-devcontainer-skeleton

895d43ebb4 | 3 branches | 3 tags | Go to file | Code

clearbluejar first simple_diff — 895d43e on Aug 15, 2022 — 4 commits

.devcontainer	update to allow native Ghidra binary building	last year
.ghidra_projects	Initial commit	last year
.vscode	Initial commit	last year
.gitignore	Initial commit	last year
LICENSE	Initial commit	last year
README.md	first simple_diff	last year
requirements.txt	Initial commit	last year
simple_diff.py	first simple_diff	last year

README.md

ghidra-simple-diff-engine

A Ghidra Headless (non-GUI) Python script to automate binary patch diffing.

Features

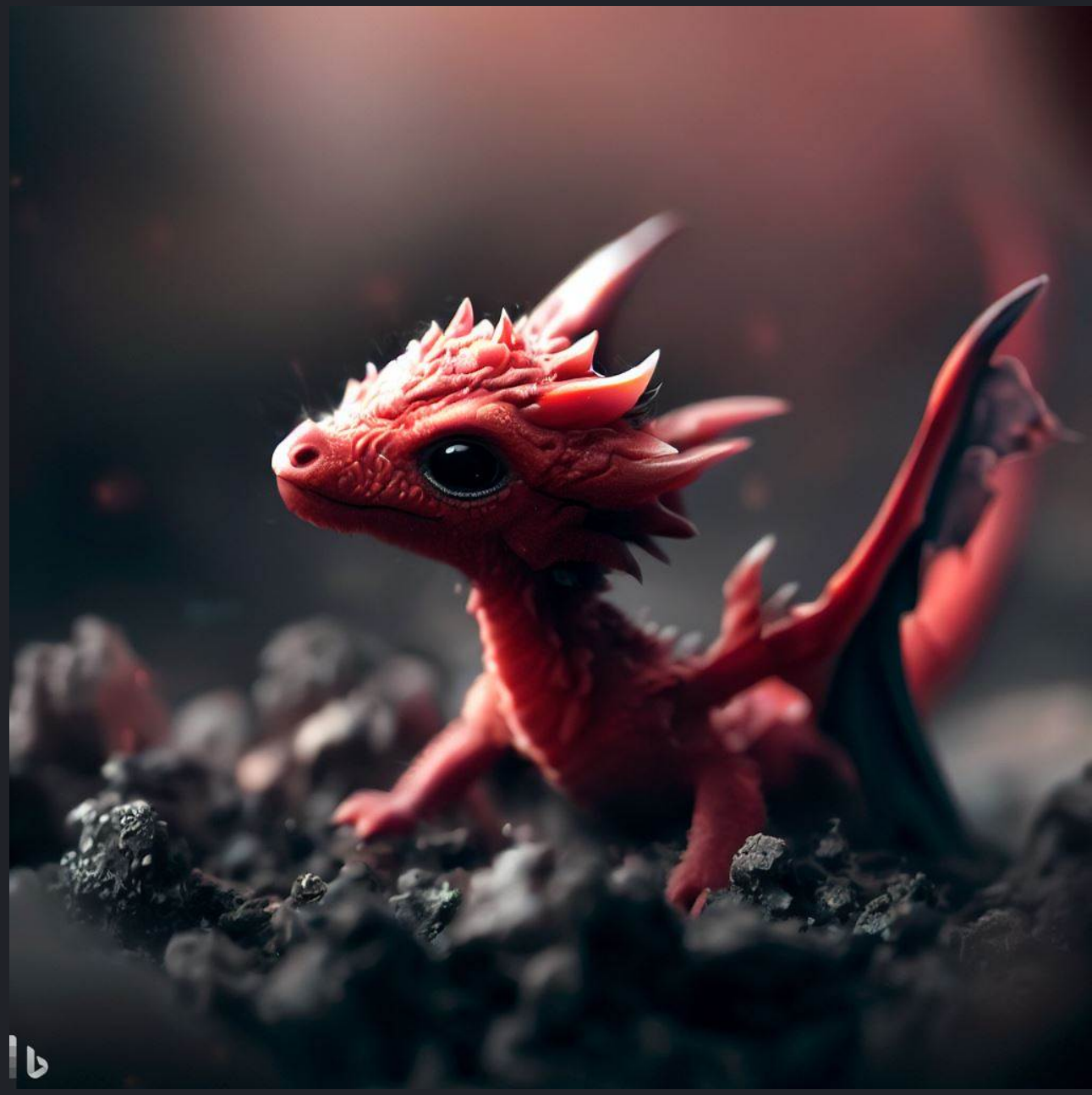
- Prescribes workflow to get you started (modify as needed)
- Container dependencies captured in .devcontainer
  - Leverages vscode python3 devcontainer image with Java feature added for running Ghidra
  - Provisions specified versions Ghidra based on `GHIDRA_VERSION` in devcontainer.json
- Auto complete for Ghidra Python script setup and configured
  - via pyi typings from VDOO-Connected-Trust/ghidra-pyi-generator
- IDE debugging (available from either)
  - justfoxing/ghidra_bridge over RPC
  - pyhidra leveraging native CPython interpreter using jpype
- Demonstrates running python scripts in various ways.

Design Goals

Perform binary diff

- Find added funcitons
- Find deleted functions
- Find modified functions
- Generate JSON capturing Diff Results

`ghidriff` was born out of both **necessity** and **curiosity**



Necessity

(aka overcoming pain points)

Workflow

Standard Binary Diffing Workflow

1. Obtain two binaries to diff (patched and vulnerable)
2. Create new SRE project
3. Import old and new binary
4. Run analysis on binaries
5. Run diffing heuristics
6. Export the analysis for each file
7. Open up the exported analysis in the corresponding diff tool
8. Analyze the diff

```
ghidriff old.dll new.dll
```

`ghidriff` changes the workflow to 3 steps

1. Download two binaries to diff
2. Run `ghidriff old.bin new.bin`
3. Analyze the diff

Decompilation Diffs

Version Tracking (SOURCE TOOL): WindowsPrintSpooler:/2020-04/p..ooler-core-localspl_6.1.7601.24383/localspl.dll

File Edit Analysis Graph Navigation Search Select Tools Window Help

Program Trees

- localspl.dll
  - Headers
  - .text
  - .rdata
  - .data
  - .pdata
  - .rsrc
  - .reloc
  - Debug Data

Program Tree

Data Type Manager

- Data Types
  - BuiltInTypes
  - localspl.dll
  - winapi_64
  - windows_vs12_64

Filter:

Listing: localspl.dll

```
                    undefined4          Stack[0x10]:4  local_res10

                    undefined8          Stack[0x8]:8   local_res8

                    undefined8          Stack[-0x38]:8 local_38

                                  ?GetPrinterSize@@YAKPEAU_INIPRINT
                                  GetPrinterSize
7ff76f0159c 48 89 5c        MOV        qword ptr [RSP +
            24 08
7ff76f015a1 48 89 6c        MOV        qword ptr [RSP +
            24 18
7ff76f015a6 48 89 74        MOV        qword ptr [RSP +
            24 20
7ff76f015ab 57              PUSH       RDI
7ff76f015ac 41 54           PUSH       R12
7ff76f015ae 41 55           PUSH       R13
7ff76f015b0 41 56           PUSH       R14
7ff76f015b2 41 57           PUSH       R15
7ff76f015b4 48 83 ec 30     SUB        RSP,0x30
7ff76f015b8 33 db           XOR        EBX,EBX
7ff76f015ba 4d 8b e9        MOV        R13,param_4
7ff76f015bd 4c 8b e1        MOV        R12,param_1
7ff76f015c0 8d 6b 01        LEA        EBP,[RBX + 0x1]
7ff76f015c3 3b d3           CMP        param_2,EBX
7ff76f015c5 0f 84 b8        JZ         LAB_7ff76f1fb83
            e5 01 00
7ff76f015cb 2b d5           SUB        param_2,EBP
7ff76f015cd 0f 84 6c        JZ         LAB_7ff76f1c63f
```

Decompile: GetPrinter...

```
/* unsigned long __cdecl GetPrinterSize
   long,unsigned short * __ptr64,struct

uint GetPrinterSize(longlong param_1,in

{
  short sVar1;
  DWORD DVar2;
  int iVar3;
  longlong lVar4;
  int iVar5;
  uint uVar6;
  int iVar7;
  short *psVar8;
  int iVar9;
  int iVar10;
```

Version Tracking Matches for Source

Source Label: GetPrinterSize Label Type: Analysis Source

1	...	...	...	...	D...	Des...	2	...	...	Alg...
	...	...	2	0	Gl...	Get...	7...	...	...	Ex...
	...	...	2	0	Gl...	Get...	7...	...	...	Ex...
	...	...	2	0	Gl...	Get...	7...	...	...	Co...
	...	...	2	0	Gl...	Get...	7...	...	...	Ex...

7ff76f0159c GetPrinterSize MOV qword ptr [RSP + 0x8],RBX

Version Tracking (DESTINATION TOOL): WindowsPrintSpooler:/2020-05/p..ooler-core-localspl_6.1.7601.24554/localspl.dll

File Edit Analysis Graph Navigation Search Select Tools Window Help

Program Trees

- localspl.dll
  - Headers
  - .text
  - .rdata
  - .data

Program Tree

Data Type Manager

- Data Types
  - BuiltInTypes
  - localspl.dll
  - spooler_types
  - winapi_64
  - windows_vs12_64

Filter:

Listing: loc...

```
                    undefined8          Sta

                    undefined8          Sta

                                  ?GetP
                                  GetPr
7ff76f0159c 48 89 5c        M
            24 08
7ff76f015a1 48 89 6c        M
            24 18
7ff76f015a6 48 89 74        M
            24 20
7ff76f015ab 57              P
7ff76f015ac 41 54           P
7ff76f015ae 41 55           P
7ff76f015b0 41 56           P
7ff76f015b2 41 57           P
```

Decompile: GetPrinterSize - (localspl.dll)

```
/* unsigned long __cdecl GetPrinterSize(struct _INIPRINTER * __ptr64,u
   long,unsigned short * __ptr64,struct _devicemodeW * __ptr64) */

uint GetPrinterSize(longlong param_1,int param_2,undefined8 param_3,sh

{
  short sVar1;
  DWORD DVar2;
  int iVar3;
  longlong lVar4;
  int iVar5;
  uint uVar6;
  int iVar7;
  short *psVar8;
  int iVar9;
  int iVar10;
  int iVar11;
  int iVar12;
```

Version Tracking Matches for Destination

Destination Label: GetPrinterSize Label Type: Analysis Destination Address: 7ff76f0159c

Function Call Trees: GetPrinterSize - (localspl.dll)

Incoming Calls

- Incoming References - GetPrinterSize
  - SplEnumPrinters
  - SplGetPrinter

Outgoing Calls

- Outgoing References - GetPrinterSize
  - GetSecurityDescriptorLength
  - GetPrinterPorts

Filter:

7ff76f0159c GetPrinterSize MOV qword ptr [RSP + 0x8],RBX

source-AlpcpCreateRegion-1406be018.c ↔ dest-AlpcpCreateRegion-1406be0d8.c

C: > Users > user > AppData > Local > Temp > dest-AlpcpCreateRegion-1406be0d8.c

```c
undefined8
AlpcpCreateRegion(longlong *param_1,longlong param_2,longlong param_3,undefined8 *pa

{
  longlong **pplVar1;
  longlong **pplVar2;
  void *pvVar3;
  longlong *plVar4;
  longlong **pplVar5;
  longlong *plVar6;
  ulonglong uVar7;
  longlong **pplVar8;
  longlong **pplVar9;
  longlong *plVar10;
  longlong *plVar11;
  longlong *plVar12;
  uint uVar13;
  longlong *plVar14;

  pvVar3 = SystemReserved1[15];
  *param_4 = 0;
  if (param_1[4] != *(longlong *)((longlong)pvVar3 + 0xb8)) {
    return 0xc0000022;
  }
  uVar7 = (ulonglong)AlpcpViewGranularity;
  pplVar5 = (longlong **)(param_1 + 7);
  uVar13 = AlpcpViewGranularity - 1;
  plVar14 = (longlong *)
            ((ulonglong)(AlpcpRegionGranularity - 1) + param_3 &
            ~((ulonglong)AlpcpRegionGranularity - 1));
```

```c
undefined8
AlpcpCreateRegion(longlong *param_1,longlong param_2,longlong *param_3,undefined8 *p

{
  longlong **pplVar1;
  longlong **pplVar2;
  void *pvVar3;
  longlong *plVar4;
  longlong *plVar5;
  longlong **pplVar6;
  longlong **pplVar7;
  longlong **pplVar8;
  longlong *plVar9;
  longlong *plVar10;
  longlong *plVar11;
  longlong *plVar12;
  longlong *plVar13;

  pvVar3 = SystemReserved1[15];
  *param_4 = 0;
  if (param_1[4] != *(longlong *)((longlong)pvVar3 + 0xb8)) {
    return 0xc0000022;
  }
  plVar12 = (longlong *)
            ((ulonglong)(AlpcpViewGranularity - 1) + (longlong)param_3 &
            ~((ulonglong)AlpcpViewGranularity - 1));
  plVar13 = (longlong *)
            ((ulonglong)(AlpcpRegionGranularity - 1) + (longlong)param_3 &
            ~((ulonglong)AlpcpRegionGranularity - 1));
  if ((plVar12 < param_3) || (plVar13 < param_3)) {
    return 0xc000000d;
  }
  pplVar6 = (longlong **)(param_1 + 7);
```

Sharing Results

Most tools have the results exportable as images or only available within the tool GUI

Needed an easy way to share results...

Markdown Implementations

- Microsoft Teams
- Discord
- JotterPad
- Doxygen
- RStudio
- GitHub Flavored Markdown
- RMarkdown
- Nextcloud Notes
- Simplenote
- Obsidian
- Mozilla Thunderbird
- Kanboard
- Discourse
- Bugzilla
- GitLab
- Every blogging platform
- Many more..

Markdown All The Things

If you don't know already, I am a huge fan of markdown and `mermaidjs`.

> I write my notes (and most everything) in Markdown, along with what seems to be most of the rest of the world. While using Markdown, I discovered Mermaids.js for charts and graphs and haven't looked back. 2022-03-19-introducing-cve-markdown-charts-part-1

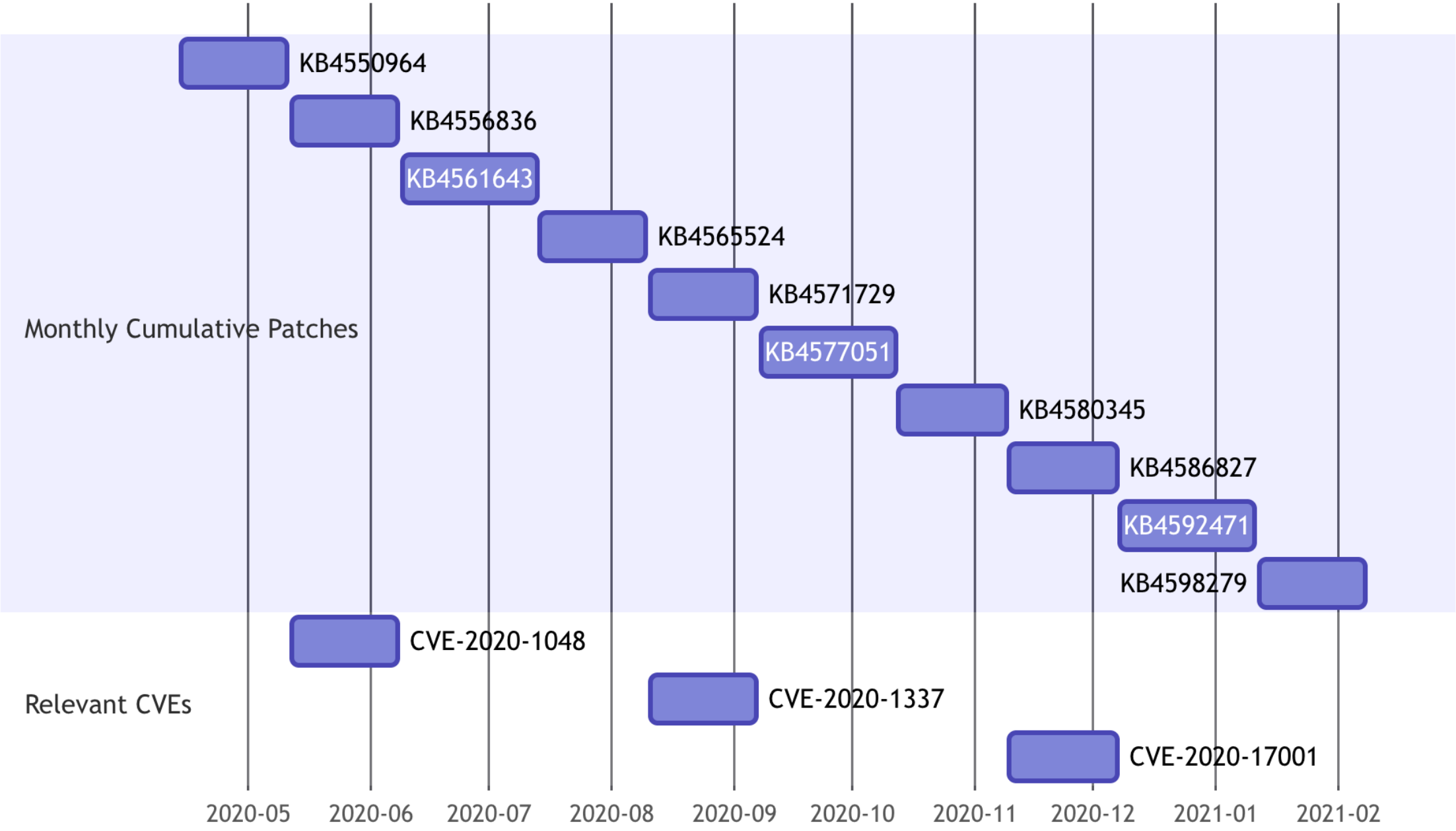
I have created several projects for which the primary output of the project is markdown, with ghidra-pyhidra-callgraphs being no exception. It order to do that, I had to translate my `CallGraph` class to a format that `mermaidjs` would understand.

Callgraphs with Ghidra, Pyhidra, and Jpype

Markdown

```mermaid
gantt

title Windows Print Spooler (6.1.7601) Monthly Patches and CVEs
dateFormat  YYYY-MM-DD
axisFormat %Y-%m

section Monthly Cumulative Patches
KB4550964 :m1, 2020-04-14, 2020-05-11
KB4556836 :m2, 2020-05-12, 2020-06-08
KB4561643 :m3, 2020-06-09, 2020-07-13
KB4565524 :m4, 2020-07-14, 2020-08-10
KB4571729 :m5, 2020-08-11, 2020-09-07
KB4577051 :m6, 2020-09-08, 2020-10-12
KB4580345 :m7, 2020-10-13, 2020-11-09
KB4586827 :m8, 2020-11-10, 2020-12-07
KB4592471 :m9, 2020-12-08, 2021-01-11
KB4598279 :m10, 2021-01-12, 2021-02-08

```

Windows Print Spooler (6.1.7601) Monthly Patches and CVEs



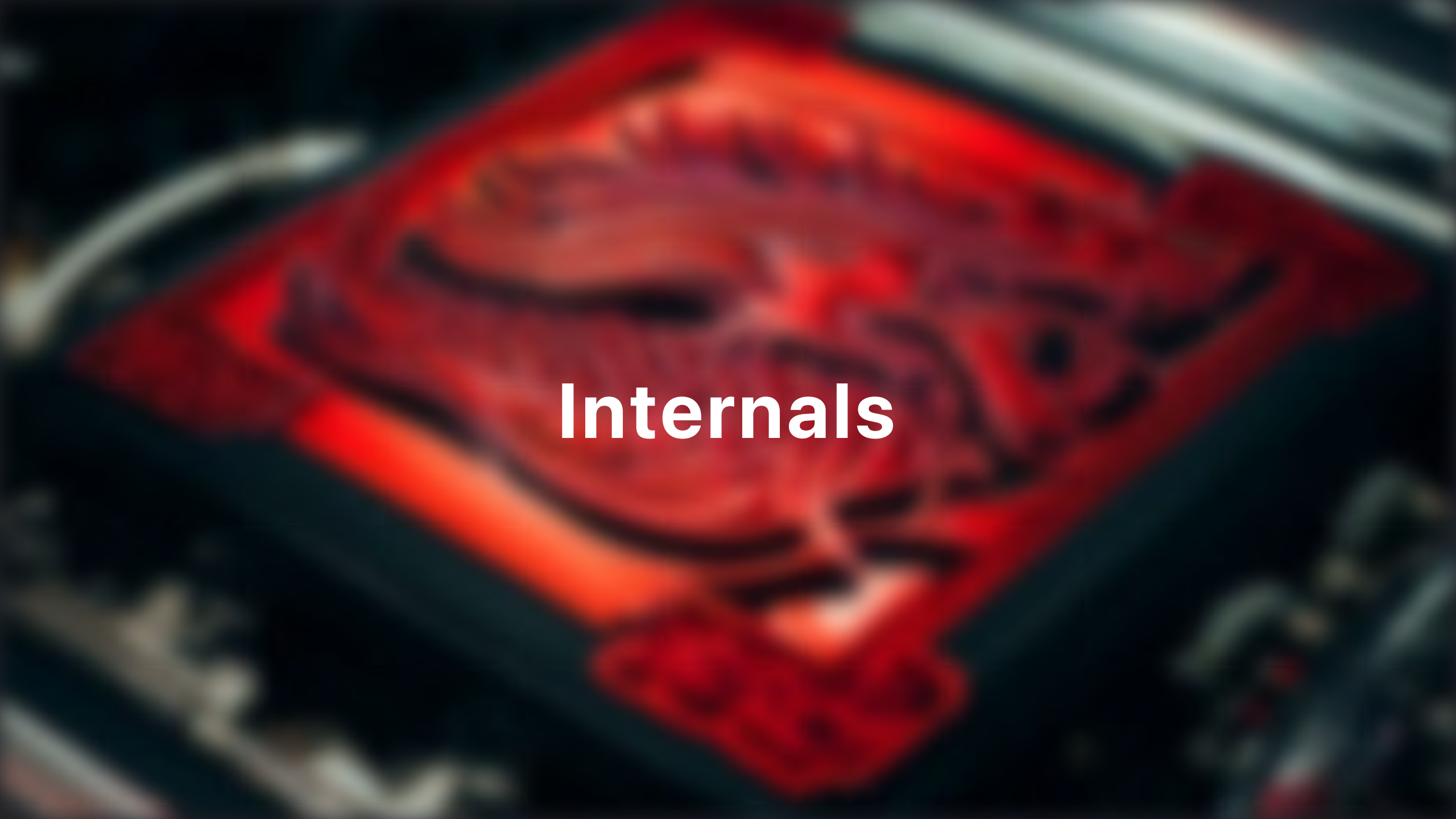
Curiosity

“ Curiosity is the wick in the candle of learning. ”

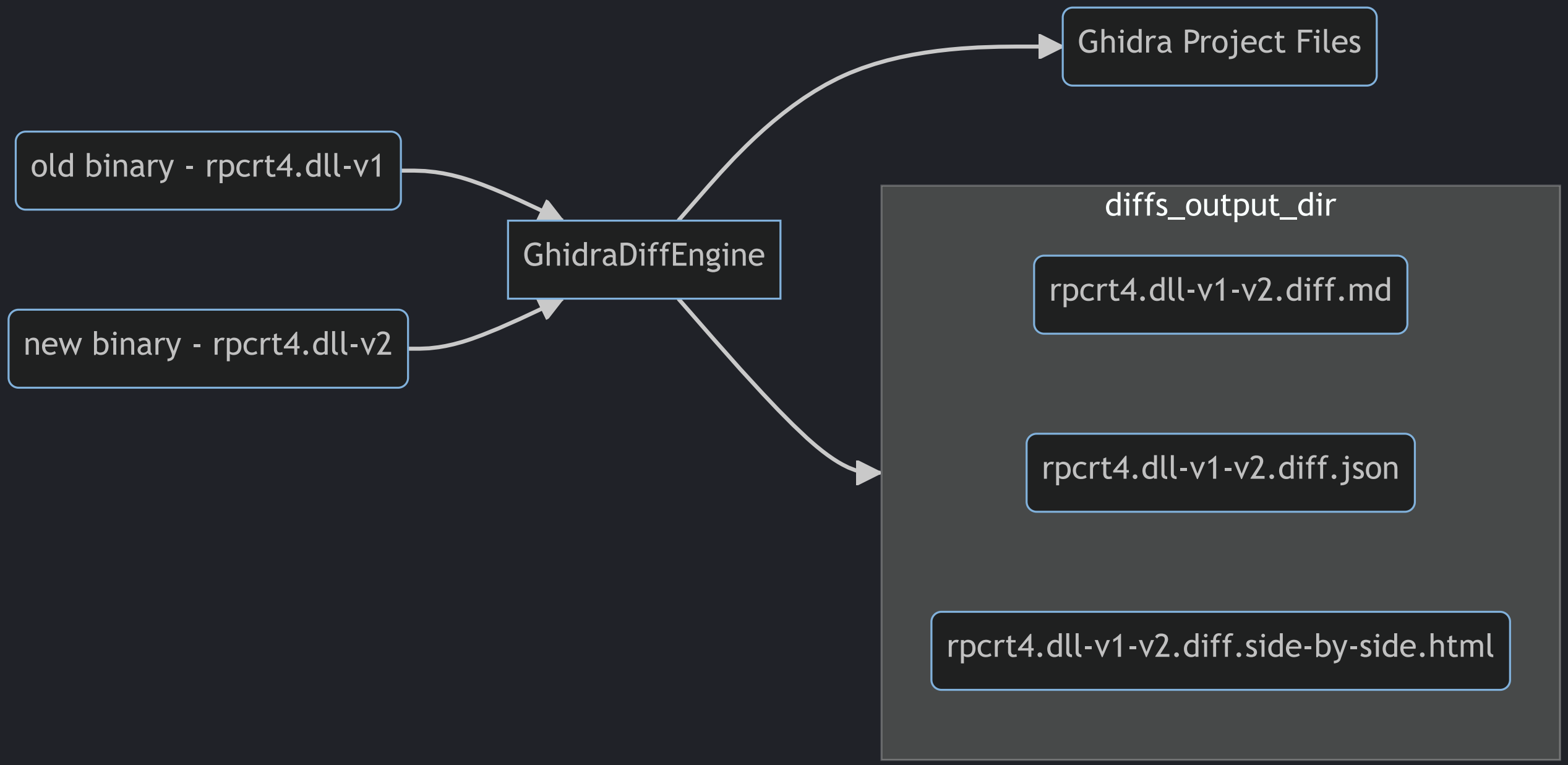
William Arthur Ward

Writing Your Own Tooling

- Understand and appreciate complexity
- Gain insight into what is important vs nice to have
- Able to mitigate pain points
- Ghidra internals knowledge++



Internals


Ghidra Project Files
old binary - rpcrt4.dll-v1
GhidraDiffEngine
new binary - rpcrt4.dll-v2
diffs_output_dir
rpcrt4.dll-v1-v2.diff.md
rpcrt4.dll-v1-v2.diff.json
rpcrt4.dll-v1-v2.diff.side-by-side.html

Design Goals

- Find all added, deleted, and modified functions
- Simple, Fast, Accurate
- Resilient
- Extendable
- Easy sharing of results
- Social Diffing

Design Choices

Ghidra

- Free / Open Source
- Great support
- Constant improvements
- Rich Programming API

Simple - Code

main | 3 branches | 3 tags | Go to file | Add file | Code

clearbluejar update readme — 90d3f04 40 minutes ago — 124 commits

.devcontainer	update readme	40 minutes ago
.github/workflows	switch workflow triggers to main	yesterday
.vscode	update readme	40 minutes ago
ghidriff	move get_parser, bump ver, add testing in setup.cfg	yesterday
tests	fix test data git clone	yesterday
.gitignore	use test data repo for dev and tests	yesterday
LICENSE	Initial commit	last year
README.md	update readme	40 minutes ago
setup.cfg	move get_parser, bump ver, add testing in setup.cfg	yesterday
setup.py	convert to python package	last year

ghidriff / ghidriff /

Add file

clearbluejar move get_parser, bump ver, add testing in setup.cfg ✕ 6f3f98c · yesterday History

Name	Last commit message	Last commit date
..		
__init__.py	move get_parser, bump ver, add testing in setup.cfg	yesterday
__main__.py	move get_parser, bump ver, add testing in setup.cfg	yesterday
correlators.py	move vt_session to new branch	3 days ago
ghidra_diff_engine.py	add pe download urls #38	3 months ago
implied_matches.py	refactor implied correlator	3 months ago
markdown.py	add pe download urls #38	3 months ago
simple_diff.py	delete unused code	6 months ago
structural_graph_diff.py	delete unused code	6 months ago
utils.py	add pe download urls #38	3 months ago
version_tracking_diff.py	move vt_session to new branch	3 days ago

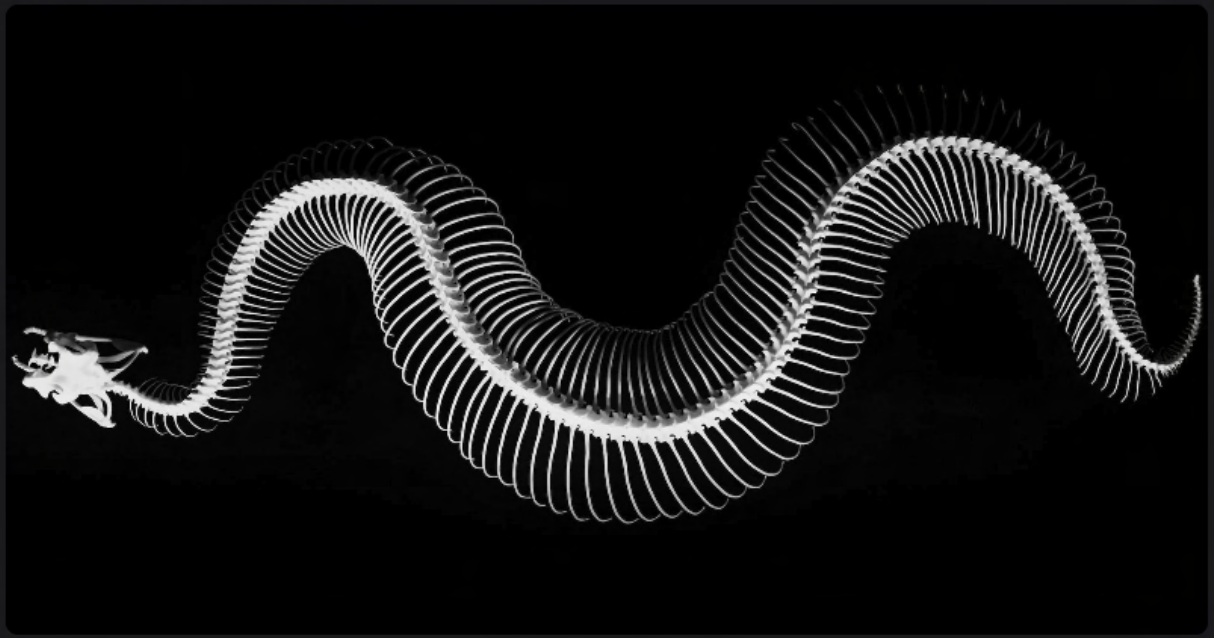
`ghidriff` Main

1. Parse arguments
2. Setup Ghidra project
3. Analyze Binaries
4. Diff binaries
5. Generate Markdown

Simple - Orchestrating Ghidra via Python

Ghidra Python Paleontology

Posted Sep 29, 2022 • Updated Jul 2, 2023



Ghidra Python Skeleton

By clearbluejar

15 min read

TL;DR - This post will walk through the process of creating a Headless Ghidra Python VScode template. This is not recommended as the official language for Ghidra is Java and the supported IDE is Eclipse, but we will give it a go. The process involved "digging up" the Ghidra Python Scripting landscape and understanding what was possible. The lessons learned are capture in the VScode template ghidra-python-vscode-devcontainer-skeleton that alleviates the pain of getting setup with Ghidra Python scripting and leverages the power of devcontainers.

Recently Updated

Ghidra Python Paleontology

Callgraphs with Ghidra, Pyhidra, and Jpy…

Desuperpacking Meta Superpacked APKs

Introducing CVE North Stars

These Are Your First Steps

Trending Tags

ghidra python cve docker graphs markdown mermaidjs NTLMrelay ntobjectmanager rpc

Contents

Pyhidra

Pyhidra is a Python library that provides direct access to the Ghidra API within a native CPython interpreter using jpype.

python automation malware-analysis malware-research ghidra

Readme

View license

Activity

107 stars

6 watching

12 forks

#SecTorCA2023

```python
import pyhidra

with pyhidra.open_program("binary_file.exe") as flat_api:
    program = flat_api.getCurrentProgram()
    listing = program.getListing()
    print(listing.getCodeUnitAt(flat_api.toAddr(0x1234)))

    # We are also free to import ghidra while in this context to do more advanced things.
    from ghidra.app.decompiler.flatapi import FlatDecompilerAPI
    decomp_api = FlatDecompilerAPI(flat_api)
    # ...
    decomp_api.dispose()
```

JPype

implementation	cpython
python	3.7 | 3.8 | 3.9 | 3.10
java	8 | 9 | 11
jvm	Open | Oracle | Corretto
platform	linux-ppc64le | osx-arm64 | linux-64 | win-32 | linux-aarch64 | osx-64 | win-64
license	not identifiable by github

JPype is a Python module to provide full access to Java from within Python. It allows Python to make use of Java only libraries, exploring and visualization of Java structures, development and testing of Java libraries, scientific computing, and much more. By gaining the best of both worlds using Python for rapid prototyping and Java for strong typed production code, JPype provides a powerful environment for engineering and code development.

Fast

Jpype

“ Unlike Jython, JPype does not achieve this by re-implementing Python, but instead by interfacing both virtual machines at the native level. **This shared memory based approach achieves good computing performance**, while providing the access to the entirety of CPython and Java libraries. https://jpype.readthedocs.io/en/latest/ ”

```
92.2%]   4[
98.6%]   5[
96.5%]   6[
100.0%]  7[
7.53G/15.6G] Tasks: 48, 206 thr, 0 kthr; 8 running
2.16M/4.00G] Load average: 8.99 5.28 2.33
             Uptime: 1 day, 01:15:55

s▽MEM%   TIME+   Command
7  0.8  1:09.85 /ghidra/Ghidra/Features/Decompiler/build/os/linux_arm_64/decompil
9  0.4  1:03.31 /ghidra/Ghidra/Features/Decompiler/build/os/linux_arm_64/decompil
5  0.7  0:36.38 /ghidra/Ghidra/Features/Decompiler/build/os/linux_arm_64/decompil
2  0.8  1:05.36 /ghidra/Ghidra/Features/Decompiler/build/os/linux_arm_64/decompil
0 13.9  9:56.76 /workspaces/ghidriff/.env/bin/python -X frozen_modules=off /home/
5  0.5  1:11.81 /ghidra/Ghidra/Features/Decompiler/build/os/linux_arm_64/decompil
4  0.8  1:05.92 /ghidra/Ghidra/Features/Decompiler/build/os/linux_arm_64/decompil
4  0.6  1:36.63 /ghidra/Ghidra/Features/Decompiler/build/os/linux_arm_64/decompil
5  0.8  0:57.10 /ghidra/Ghidra/Features/Decompiler/build/os/linux_arm_64/decompil
8  0.8  1:05.39 /ghidra/Ghidra/Features/Decompiler/build/os/linux_arm_64/decompil
1  0.7  0:51.29 /ghidra/Ghidra/Features/Decompiler/build/os/linux_arm_64/decompil
```

Extendable

GhidraDiffEngine

> An "engine" is a self-contained, but externally-controllable, piece of code that encapsulates powerful logic designed to perform a specific type of work.

StackOverflow - Difference between and engine and a framework

The base class implements first 3 steps of the Ghidra headless workflow:

1. **Create Ghidra Project** - Directory and collection of Ghidra project files and data
2. **Import Binary to project** - Import one or more binaries to the project for analysis
3. **Analyze Binary** - Ghidra will perform default binary analysis on each binary

```python
class NewDiffTool(GhidraDiffEngine):

    def __init__(self,verbose=False) -> None:
        super().__init__(verbose)

    @abstractmethod
    def find_matches(
            self,
            old: Union[str, pathlib.Path],
            new: Union[str, pathlib.Path]
    ) -> dict:
        """My amazing differ"""

        # find added, deleted, and modified functions
        # <code goes here>

        return [unmatched, matched]
```

Evolution of Differs

1. SimpleDiff - "Simple" as in it relies mostly on known symbols to find the differences between functions
2. StructualGraphDiff - Adds to simple using structural graph hashing
3. VersionTrackingDiff - The latest differ, with advanced several correlators function matching

```python
class SimpleDiff(GhidraDiffEngine):
    """
    An Ghidra Diff implementation using simple comparison mechanisms
    """

    def find_matches(
        self,
        p1: "ghidra.program.model.listing.Program",
        p2: "ghidra.program.model.listing.Program",
        ignore_FUN: bool = False,
    ) -> dict:
        """
        Find matching and unmatched functions between p1 and p2
        """
```

Simple Diff Function Matching

- Symbol Name
- Name + Function Length
- Address + Length
- Param Length + Length

```python
def _syms_match(esym, esym2) -> Tuple[bool, str]:
    found = False
    match_type = None
    min_func_length = 15

    if esym2['name'] == esym['name'] and esym2['length'] == esym['length']:
        self.logger.info("Name + length {} {}".format(sym.getName(True), sym2.getName(True)))
        found = True
        match_type = 'Name:Length'
    elif esym2['address'] == esym2['address'] and esym2['length'] == esym['length'] and min([esym['length'], esym2['length']]) > min_func_length:
        self.logger.info("Address + Length {} {}".format(sym.getName(True), sym2.getName(True)))
        found = True
        match_type = 'Address:Length'
    elif esym2['paramcount'] == esym['paramcount'] and esym2['length'] == esym['length']:
        self.logger.info("param count + func len {} {}".format(sym.getName(True), sym2.getName(True)))
        found = True
        match_type = 'Param:Length'
    elif esym2['fullname'] == esym['fullname']:
        self.logger.info("Name Exact {} {}".format(sym.getName(True), sym2.getName(True)))
        found = True
        match_type = 'Fullname'

    return found, match_type
```

Structural Graph Diff Function Matching

- Previous Simple Diff Heuristics
- Structural Correlator

```python
class StructualGraphDiff(GhidraDiffEngine):
    def find_matches(
        def _get_compare_key(sym: 'ghidra.program.model.symbol.Symbol', func: 'ghidra.program.model.listing.Function') -> tuple:
            """
            Builds structural graph hash. Thank you Halvar Flake!)
            """

            from ghidra.program.model.block import BasicBlockModel
            from ghidra.util.task import ConsoleTaskMonitor

            # graph structure vars
            num_basic_blocks = 0
            num_edges_of_blocks = 0
            num_call_subfunctions = 0

            if (not func.isThunk() and func.getBody().getNumAddresses() >= 10):

                monitor = ConsoleTaskMonitor()

                basic_model = BasicBlockModel(func.getProgram(), True)
                basic_blocks = basic_model.getCodeBlocksContaining(func.getBody(), monitor)

                for block in basic_blocks:
                    num_edges_of_blocks += block.getNumDestinations(monitor)
                    num_basic_blocks += 1

                    code_units = func.getProgram().getListing().getCodeUnits(block, True)
                    for code in code_units:
                        if code.getMnemonicString() == 'CALL':
                            num_call_subfunctions += 1
```

Version Tracking Diff Function Matching

```
# tuples of correlators instances
# ( name, hasher, one_to_one, one_to_many)
# DO NOT CHANGE ORDER UNLESS INTENDED, ORDER HAS MAJOR IMPACT ON ACCURACY AND EFFICIENCY
func_correlators = [
    ('ExactBytesFunctionHasher', ExactBytesFunctionHasher.INSTANCE, True, False),
    ('ExactInstructionsFunctionHasher', ExactInstructionsFunctionHasher.INSTANCE, True, False),
    (StructuralGraphExactHasher.MATCH_TYPE, StructuralGraphExactHasher(), True, False),
    ('ExactMnemonicsFunctionHasher', ExactMnemonicsFunctionHasher.INSTANCE, True, False),
    (BulkInstructionsHasher.MATCH_TYPE, BulkInstructionsHasher(), True, False),
    (SigCallingCalledHasher.MATCH_TYPE, SigCallingCalledHasher(), True, False),
    (StringsRefsHasher.MATCH_TYPE, StringsRefsHasher(), True, False),
    (StrUniqueFuncRefsHasher.MATCH_TYPE, StrUniqueFuncRefsHasher(), True, False),
    (SwitchSigHasher.MATCH_TYPE, SwitchSigHasher(), True, False),
    # WARN: one_to_many=True flag allows for false negatives is structal graph matching. Mitgated by
    (StructuralGraphHasher.MATCH_TYPE, StructuralGraphHasher(), True, True),
    # WARN: one_to_many=True flag allows for false negatives
    (BulkBasicBlockMnemonicHasher.MATCH_TYPE, BulkBasicBlockMnemonicHasher(), True, True),

    (SigCallingCalledHasher.MATCH_TYPE, SigCallingCalledHasher(), True, False),
    (StringsRefsHasher.MATCH_TYPE, StringsRefsHasher(), True, False),
    (StrUniqueFuncRefsHasher.MATCH_TYPE, StrUniqueFuncRefsHasher(), True, False),
    (SwitchSigHasher.MATCH_TYPE, SwitchSigHasher(), True, False),
]
```

Correlators

```python
@ JImplements(FunctionHasher, deferred=True)
class BulkBasicBlockMnemonicHasher:
    """
    Hash from function basic blocks mnemonics sorted
    Order of basic blocks mnemonics is ignored
    Based on https://github.com/threatrack/ghidra-patchdiff-correlator#bulk-basic-block-mnemonics-match
    """

    MIN_FUNC_LEN = 10
    MATCH_TYPE = 'BulkBasicBlockMnemonicHash'

    @ JOverride
    def hash(self, func: 'ghidra.program.model.listing.Function', monitor: 'ghidra.util.task.TaskMonitor') -> int:

        from ghidra.program.model.block import BasicBlockModel

        basic_model = BasicBlockModel(func.getProgram(), True)
        basic_blocks = basic_model.getCodeBlocksContaining(func.getBody(), monitor)
        blocks = []

        for block in basic_blocks:
            code_units = func.getProgram().getListing().getCodeUnits(block, True)
            for code in code_units:
                blocks.append(code.getMnemonicString())

        return hash(tuple(sorted(blocks)))
```

Resilient

- GitHub Actions for CI
  - Automated pytest
  - Package Building
- Docker / devcontainers
  - Test across versions and environments

clearbluejar / ghidriff

Code | Issues 16 | Pull requests | Actions | Projects 1 | Security | Insights | Settings

Actions

New workflow

All workflows

Lint Python Package

Pytest Python Package In Devcontainer

Management

Caches

Runners Beta

All workflows

Showing runs from all workflows

22 workflow runs

ignore .ds_store
Pytest Python Package In Devcontainer #15: Commit bce34e6 pushed by clearbluejar — main

ignore .ds_store
Lint Python Package #7: Commit bce34e6 pushed by clearbluejar — main

refactor imports
Lint Python Package #6: Commit 49e20ea pushed by clearbluejar — main

refactor imports
Pytest Python Package In Devcontainer #14: Commit 49e20ea pushed by clearbluejar — main

← Pytest Python Package In Devcontainer

adding pypi publish workflow #16

Re-run all jobs

Summary

Jobs

- test (latest)
- test (10.1.5ghidra3.11python-...

Run details

- Usage
- Workflow file

test (latest)

succeeded 3 weeks ago in 4m 1s

Search logs

Set up job	2s
Run actions/checkout@v3	1s
Test with pytest on devcontainer	3m 54s
Post Test with pytest on devcontainer	0s
Post Run actions/checkout@v3	0s
Complete job	0s

Sharing Results

ghidriffs > json > {} ntoskrnl.exe.10.0.22621.1344-ntoskrnl.exe.10.0.22621.1413_diff.json > {} program


```
1   {
2   >   "program_options": {…
335     },
336 >   "stats": {…
369     },
370 >   "symbols": {…
395     },
396 >   "strings": {…
417     },
418     "functions": {
419         "added": [
420             {
421                 "name":
                    "Feature_MSRC76458_DisableTransactedRename__private_IsEnable
                    d",
422                 "fullname":
                    "Feature_MSRC76458_DisableTransactedRename__private_IsEnable
                    d",
423                 "parent": "Global",
424                 "refcount": 2,
```

Social Diffing

clearbluejar / ntoskrnl.exe.10.0.22621.1344-ntoskrnl.exe.10.0.22621.1413.diff.md Secret

Last active 3 minutes ago

Edit Delete Star 0

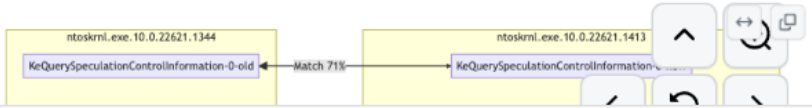
Code Revisions 2 Download ZIP

ntoskrnl.exe.10.0.22621.1344-ntoskrnl.exe.10.0.22621.1413.diff.md Raw

ntoskrnl.exe.10.0.22621.1344-10.0.22621.1413 Diff

TOC

Visual Chart Diff



ghidriff

Edited just now

Clone

ntoskrnl.exe.x64.10.0.22621.1105-ntoskrnl.exe.x64.10.0.22621.1194.diff.md 497.20 KiB

ntoskrnl.exe.x64.10.0.22621.1105-ntoskrnl.exe.x64.10.0.22621.1194 Diff

TOC

SSECURITY_CONTEXT::~SSECURITY_CONTEXT Called Diff

```
--- SSECURITY_CONTEXT::~SSECURITY_CONTEXT called
+++ SSECURITY_CONTEXT::~SSECURITY_CONTEXT called
@@ -2,0 +3 @@
+SSECURITY_CONTEXT::DeletePac
```

SSECURITY_CONTEXT::~SSECURITY_CONTEXT Diff

```
--- SSECURITY_CONTEXT::~SSECURITY_CONTEXT
+++ SSECURITY_CONTEXT::~SSECURITY_CONTEXT
@@ -1,30 +1,31 @@

 /* protected: __cdecl SSECURITY_CONTEXT::~SSECURITY_CONTEXT(void) __ptr64 */

 void __thiscall SSECURITY_CONTEXT::_SSECURITY_CONTEXT(SSECURITY_CONTEXT *this)

 {
   uint uVar1;
   char *pcVar2;
   undefined7 in_register_00000081;

+  DeletePac(this);
   uVar1 = 0;
   if (DAT_0 != 0) {
     pcVar2 = "HbBrn";
     do {
       if (*pcVar2 == 's') goto LAB_1;
       uVar1 = uVar1 + 1;
       pcVar2 = pcVar2 + 1;
```

All gists 97 | Forked 2 | Starred 3

Type: All | Sort: Recently created

clearbluejar / ntoskrnl.exe.x64.10.0.22621.1105-ntoskrnl.exe.x64.10.0.22621.1194.diff.md Secret

Created 1 hour ago

1 file | 0 forks | 0 comments | 0 stars

ntoskrnl.exe.x64.10.0.22621.1105-ntoskrnl.exe.x64.10.0.22621.1194 Diff

TOC

clearbluejar / CVE-2023-21768.md Secret

Created 7 hours ago

1 file | 0 forks | 0 comments | 0 stars

afd.sys.x64.10.0.22621.1028-afd.sys.x64.10.0.22621.1415 Diff

TOC

layout	title	parent
default	rpcrt4.dll.x64.10.0.22000.1630-rpcrt4.dll.x64.10.0.22000.1696	file-rpcrt4.dll-22000-x64

rpcrt4.dll.x64.10.0.22000.1630-rpcrt4.dll.x64.10.0.22000.1696 Diff

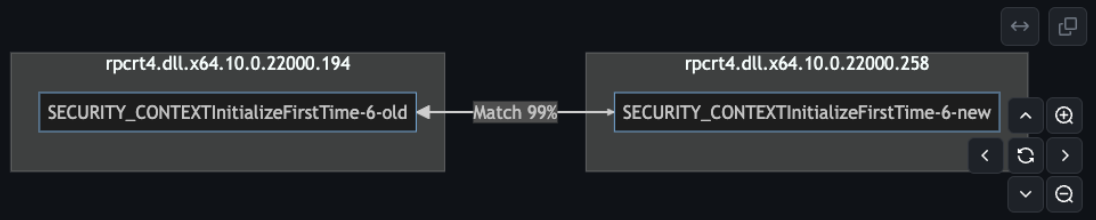
TOC

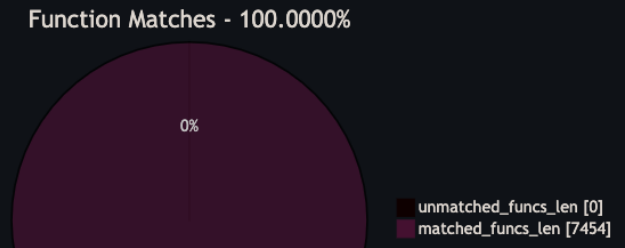
layout	title	parent
default	rpcrt4.dll.x64.10.0.22000.194-rpcrt4.dll.x64.10.0.22000.258	file-rpcrt4.dll-22000-x64

rpcrt4.dll.x64.10.0.22000.194-rpcrt4.dll.x64.10.0.22000.258 Diff

TOC

Visual Chart Diff





Features

Command Line

```
ghidriff old.bin new.bin
```

```
usage: ghidriff [-h] [--engine {SimpleDiff,StructualGraphDiff,VersionTrackingDiff}] [-o OUTPUT_PATH] [--summary SUMMARY] [-p PROJECT_LOCATION] [-n PROJECT_NAME] [-s SYMBOLS_PATH] [--threaded | --no-threaded] [--force-
analysis] [--force-diff] [--no-symbols]
                [--log-level {CRITICAL,FATAL,ERROR,WARN,WARNING,INFO,DEBUG,NOTSET}] [--file-log-level {CRITICAL,FATAL,ERROR,WARN,WARNING,INFO,DEBUG,NOTSET}] [--log-path LOG_PATH] [--va] [--max-ram-percent MAX_RAM_PERCENT]
[--print-flags] [--jvm-args [JVM_ARGS]]
                [--sxs] [--max-section-funcs MAX_SECTION_FUNCS] [--md-title MD_TITLE]
                old new [new ...]

ghidriff - A Command Line Ghidra Binary Diffing Engine

positional arguments:
  old                   Path to old version of binary '/somewhere/bin.old'
  new                   Path to new version of binary '/somewhere/bin.new'. (For multiple new binaries add oldest to newest)

options:
  -h, --help            show this help message and exit
  --engine {SimpleDiff,StructualGraphDiff,VersionTrackingDiff}
                        The diff implementation to use. (default: VersionTrackingDiff)
  -o OUTPUT_PATH, --output-path OUTPUT_PATH
                        Output path for resulting diffs (default: ghidriffs)
  --summary SUMMARY     Add a summary diff if more than two bins are provided (default: False)

Ghidra Project Options:
  -p PROJECT_LOCATION, --project-location PROJECT_LOCATION
                        Ghidra Project Path (default: .ghidra_projects)
  -n PROJECT_NAME, --project-name PROJECT_NAME
                        Ghidra Project Name (default: ghidriff)
  -s SYMBOLS_PATH, --symbols-path SYMBOLS_PATH
                        Ghidra local symbol store directory (default: .symbols)

Engine Options:
  --threaded, --no-threaded
                        Use threading during import, analysis, and diffing. Recommended (default: True)
  --force-analysis      Force a new binary analysis each run (slow) (default: False)
  --force-diff          Force binary diff (ignore arch/symbols mismatch) (default: False)
  --no-symbols          Turn off symbols for analysis (default: False)
  --log-level {CRITICAL,FATAL,ERROR,WARN,WARNING,INFO,DEBUG,NOTSET}
                        Set console log level (default: INFO)
  --file-log-level {CRITICAL,FATAL,ERROR,WARN,WARNING,INFO,DEBUG,NOTSET}
                        Set log file level (default: INFO)
  --log-path LOG_PATH   Set ghidriff log path. (default: ghidriff.log)
  --va, --verbose-analysis
                        Verbose logging for analysis step. (default: False)

JVM Options:
  --max-ram-percent MAX_RAM_PERCENT
                        Set JVM Max Ram % of host RAM (default: 60.0)
  --print-flags         Print JVM flags at start (default: False)
  --jvm-args [JVM_ARGS]
                        JVM args to add at start (default: None)

Markdown Options:
  --sxs                 Include side by side code diff (default: False)
  --max-section-funcs MAX_SECTION_FUNCS
                        Max number of functions to display per section. (default: 200)
  --md-title MD_TITLE   Overwrite default title for markdown diff (default: None)
```

```
ghidriff - A Command Line Ghidra Binary Diffing Engine

positional arguments:
  old                   Path to old version of binary '/somewhere/bin.old'
  new                   Path to new version of binary '/somewhere/bin.new'.
                        (For multiple new binaries add oldest to newest)

options:
  -h, --help            show this help message and exit
  --engine {SimpleDiff,StructualGraphDiff,VersionTrackingDiff}
                        The diff implementation to use. (default:
                        VersionTrackingDiff)
  -o OUTPUT_PATH, --output-path OUTPUT_PATH
                        Output path for resulting diffs (default: ghidriffs)
  --summary SUMMARY     Add a summary diff if more than two bins are
                        provided (default: False)
```

```
Ghidra Project Options:
  -p PROJECT_LOCATION, --project-location PROJECT_LOCATION
                        Ghidra Project Path (default: .ghidra_projects)
  -n PROJECT_NAME, --project-name PROJECT_NAME
                        Ghidra Project Name (default: ghidriff)
  -s SYMBOLS_PATH, --symbols-path SYMBOLS_PATH
                        Ghidra local symbol store directory (default:
                        .symbols)
```

```
Engine Options:
  --threaded, --no-threaded
                        Use threading during import, analysis, and diffing.
                        Recommended (default: True)
  --force-analysis      Force a new binary analysis each run (slow) (default: False)
  --force-diff          Force binary diff (ignore arch/symbols mismatch) (default:
                        False)
  --no-symbols          Turn off symbols for analysis (default: False)
  --log-level {CRITICAL,FATAL,ERROR,WARN,WARNING,INFO,DEBUG,NOTSET}
                        Set console log level (default: INFO)
  --file-log-level {CRITICAL,FATAL,ERROR,WARN,WARNING,INFO,DEBUG,NOTSET}
                        Set log file level (default: INFO)
  --log-path LOG_PATH   Set ghidriff log path. (default: ghidriff.log)
  --va, --verbose-analysis
                        Verbose logging for analysis step. (default: False)
```

```
JVM Options:
  --max-ram-percent MAX_RAM_PERCENT
                        Set JVM Max Ram % of host RAM (default: 60.0)
  --print-flags         Print JVM flags at start (default: False)
  --jvm-args [JVM_ARGS]
                        JVM args to add at start (default: None)
```

```
Markdown Options:
  --sxs                   Include side by side code diff (default: False)
  --max-section-funcs MAX_SECTION_FUNCS
                          Max number of functions to display per section. (default: 200)
  --md-title MD_TITLE     Overwrite default title for markdown diff (default: None)
```

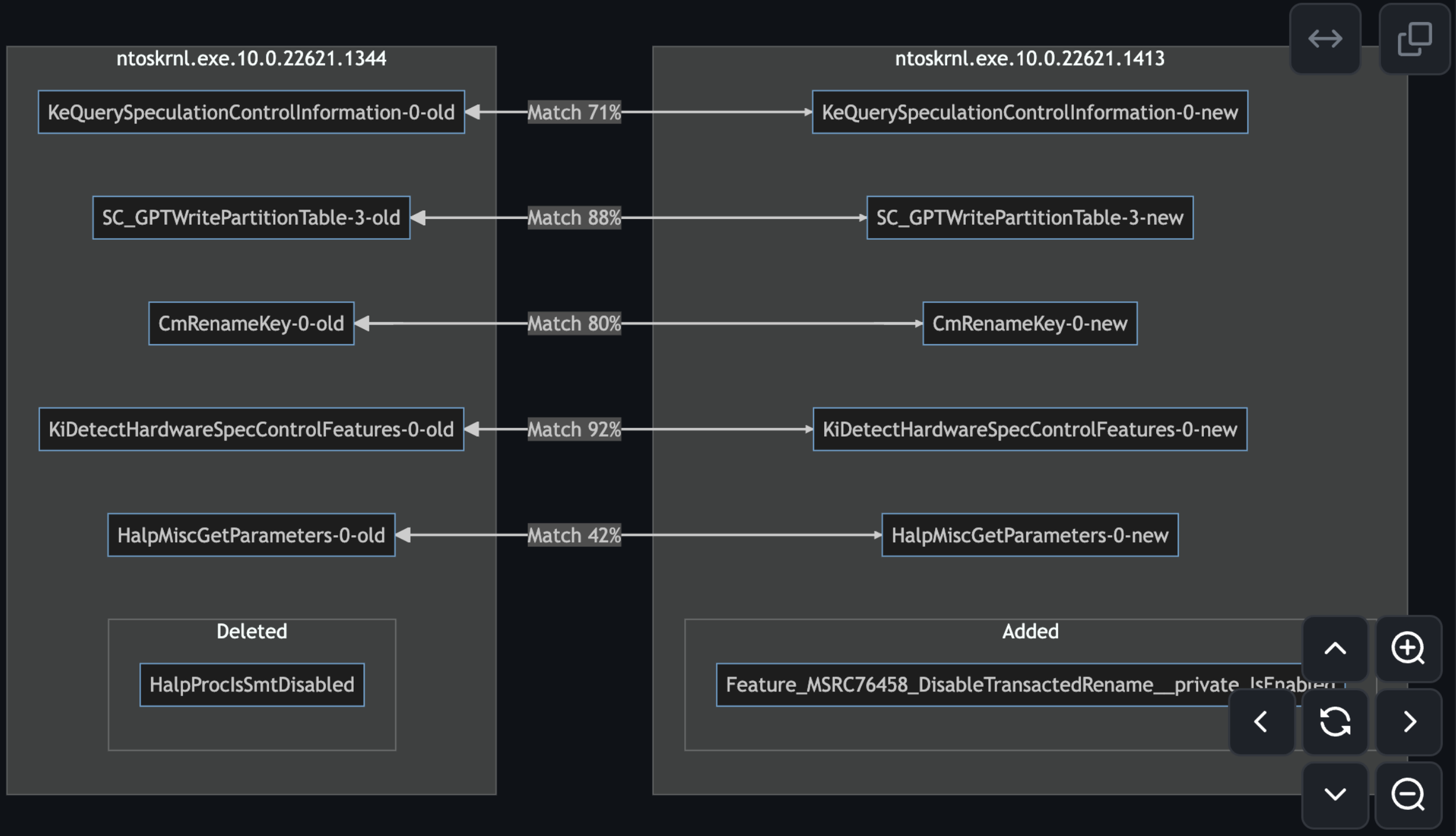
Summary TOC

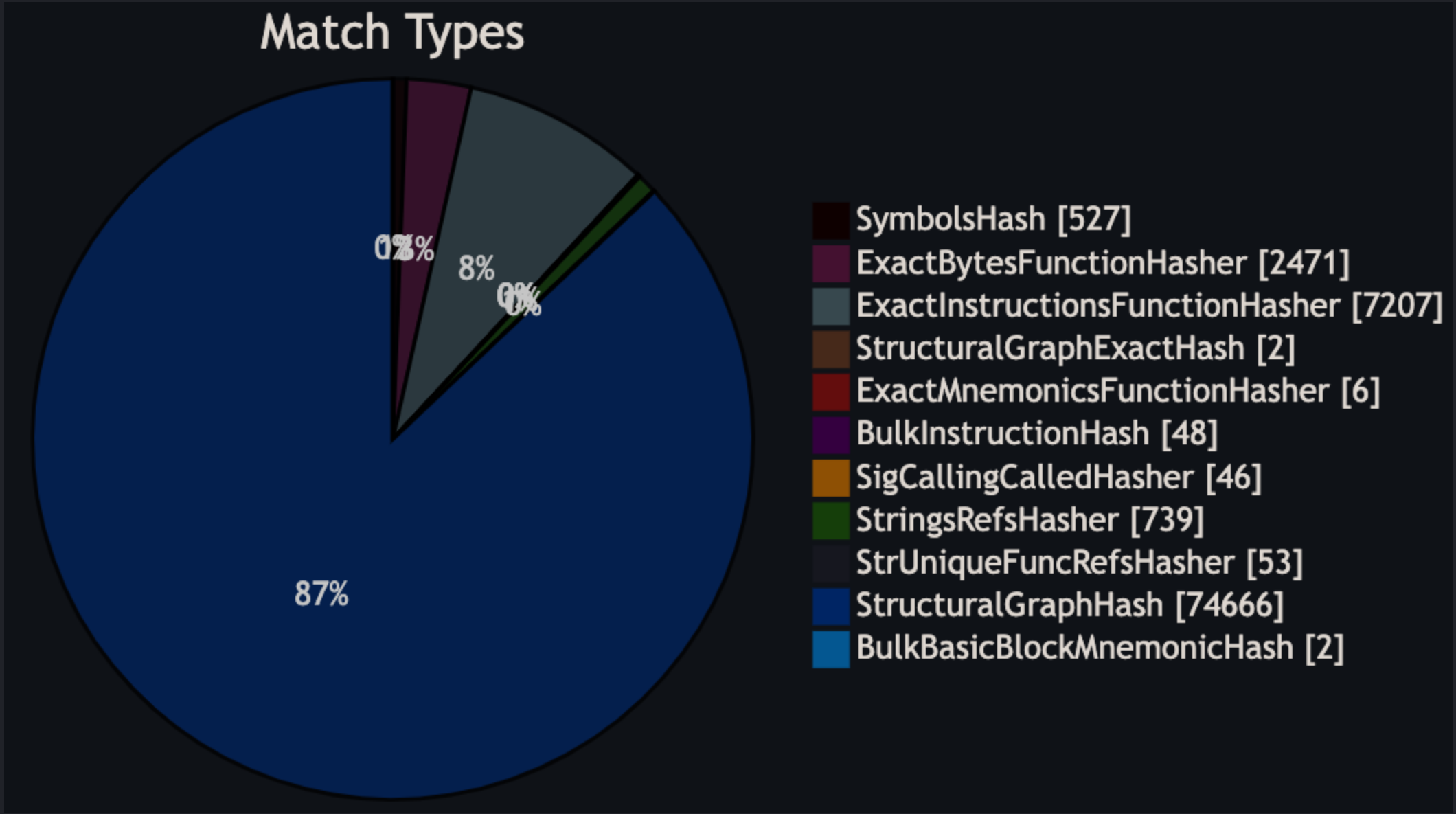
ntoskrnl.exe.10.0.22621.1344-ntoskrnl.exe.10.0.22621.1413.diff.md Raw

ntoskrnl.exe.10.0.22621.1344-10.0.22621.1413 Diff

TOC

Visual Diff Charts


ntoskrnl.exe.10.0.22621.1344
ntoskrnl.exe.10.0.22621.1413
KeQuerySpeculationControlInformation-0-old
Match 71%
KeQuerySpeculationControlInformation-0-new
SC_GPTWritePartitionTable-3-old
Match 88%
SC_GPTWritePartitionTable-3-new
CmRenameKey-0-old
Match 80%
CmRenameKey-0-new
KiDetectHardwareSpecControlFeatures-0-old
Match 92%
KiDetectHardwareSpecControlFeatures-0-new
HalpMiscGetParameters-0-old
Match 42%
HalpMiscGetParameters-0-new
Deleted
HalpProcIsSmtDisabled
Added
Feature_MSRC76458_DisableTransactedRename__private_IsEnabled


Match Types
8%
87%
SymbolsHash [527]
ExactBytesFunctionHasher [2471]
ExactInstructionsFunctionHasher [7207]
StructuralGraphExactHash [2]
ExactMnemonicsFunctionHasher [6]
BulkInstructionHash [48]
SigCallingCalledHasher [46]
StringsRefsHasher [739]
StrUniqueFuncRefsHasher [53]
StructuralGraphHash [74666]
BulkBasicBlockMnemonicHash [2]

Metadata Diffs

Binary Metadata Diff

```diff
--- ntoskrnl.exe.10.0.22621.1344 Meta
+++ ntoskrnl.exe.10.0.22621.1413 Meta
@@ -1,44 +1,44 @@
-Program Name: ntoskrnl.exe.10.0.22621.1344
+Program Name: ntoskrnl.exe.10.0.22621.1413
 Language ID: x86:LE:64:default (2.14)
 Compiler ID: windows
 Processor: x86
 Endian: Little
 Address Size: 64
 Minimum Address: 140000000
 Maximum Address: ff0000184f
 # of Bytes: 17064868
 # of Memory Blocks: 42
-# of Instructions: 2416711
-# of Defined Data: 74860
+# of Instructions: 2416732
+# of Defined Data: 74864
 # of Functions: 30350
-# of Symbols: 245680
+# of Symbols: 245683
```

```
 Compiler: visualstudio:unknown
 Created With Ghidra Version: 10.3.3
-Date Created: Tue Sep 12 03:07:06 UTC 2023
+Date Created: Tue Sep 12 03:07:13 UTC 2023
 Executable Format: Portable Executable (PE)
-Executable Location: /workspaces/ghidriff/bins/ntoskrnl.exe.10.0.22621.1344
-Executable MD5: 1984a75b49db81a4133679eca2badc11
-Executable SHA256: 1b30d5f89790f8ee0d80d2ed29d1177dd3f58042a89e9efee9be17a46
-FSRL: file:///workspaces/ghidriff/bins/ntoskrnl.exe.10.0.22621.1344?MD5=1984
+Executable Location: /workspaces/ghidriff/bins/ntoskrnl.exe.10.0.22621.1413
+Executable MD5: d36bbf54a97597dad12dc13590601783
+Executable SHA256: 140ae8fda7efff8039514b89f571e6ae27e2c634881e3d3e1dc4b4e37
+FSRL: file:///workspaces/ghidriff/bins/ntoskrnl.exe.10.0.22621.1413?MD5=d36b
 PDB Age: 1
 PDB File: ntkrnlmp.pdb
-PDB GUID: fb0913af-0585-f234-bd64-a64a87c62db1
+PDB GUID: 797e613d-b16d-b6c0-e577-95a0cb03f471
 PDB Loaded: true
 PDB Version: RSDS
 PE Property[CompanyName]: Microsoft Corporation
 PE Property[FileDescription]: NT Kernel & System
-PE Property[FileVersion]: 10.0.22621.1344 (WinBuild.160101.0800)
+PE Property[FileVersion]: 10.0.22621.1413 (WinBuild.160101.0800)
 PE Property[InternalName]: ntkrnlmp.exe
```

Strings Diff

```diff
--- deleted strings
+++ added strings
@@ -1,2 +1,4 @@
-s_2.22.16.11__001ce0be
-s_2.22.16.11_001e8b09
+s_GccNetworkControllerConfig_00192480
+s_fix_group_reordering_001828f4
+s_2.22.16.12_001de088
+s_2.22.16.12__0019e56c
```

Command Line

Known Command Line

```
python ghidriff --project-location .ghidra_projects --project-name ghidriff --symbo
```

Download Original PEs

```
wget https://msdl.microsoft.com/download/symbols/ntkrnlmp.exe/AC027CA41047000/ntkrn
wget https://msdl.microsoft.com/download/symbols/ntkrnlmp.exe/3F960EFF1047000/ntkrn
```

IoReuseIrp

Match Info

Key	ntoskrnl.exe.x64.10.0.22621.1105 - ntoskrnl.exe.x64.10.0.22621.1194
diff_type	code,length,address,called
ratio	0.89
i_ratio	0.75
m_ratio	0.98
b_ratio	1
match_types	SymbolsHash

Function Meta Diff

Key	ntoskrnl.exe.x64.10.0.22621.1105	ntoskrnl.exe.x64.10.0.22621.1194
name	IoReuseIrp	IoReuseIrp
fullname	IoReuseIrp	IoReuseIrp
refcount	7	7
`length`	637	614
`called`	▼ Expand for full list: EtwActivityIdControl EtwWriteEx Feature_Servicing_CopyCancel_40135345__private_IsEnabled IoSetActivityIdIrp IopFreeCopyObjectsFromIrp IopIrpHasExtensionType IopIsActivityTracingEventEnabled IovpLogStackTrace VfIoInitializeIrp __security_check_cookie memset	EtwActivityIdControl EtwWriteEx IoSetActivityIdIrp IopFreeCopyObjectsFromIrp IopIrpHasExtensionType IopIsActivityTracingEventEnabled IovpLogStackTrace VfIoInitializeIrp __security_check_cookie memset
calling	PopAllocateIrp PopPrepareIoctl SmKmFileInfoCleanup	PopAllocateIrp PopPrepareIoctl SmKmFileInfoCleanup

NtCreateLowBoxToken Called Diff

```diff
--- NtCreateLowBoxToken called
+++ NtCreateLowBoxToken called
@@ -5 +4,0 @@
-Feature_Servicing_EaseTokenSACLPPLRestriction
```

IoReuseIrp Diff

```diff
--- IoReuseIrp
+++ IoReuseIrp
@@ -1,112 +1,105 @@

 void IoReuseIrp(undefined2 *param_1,undefined4 param_2)

 {
   undefined2 *puVar1;
   byte bVar2;
   undefined uVar3;
   ushort uVar4;
   undefined2 uVar5;
   bool bVar6;
   char cVar7;
   longlong lVar8;
   undefined8 unaff_retaddr;
   undefined auStack_88 [32];
   longlong local_68;
   undefined *local_60;
   undefined4 local_58;
   undefined8 local_50;
   undefined local_48 [16];
   ulonglong local_38;

-                    /* 0x347500  1038  IoReuseIrp */
+                    /* 0x3473c0  1038  IoReuseIrp */
   local_38 = __security_cookie ^ (ulonglong)auStack_88;
   bVar6 = false;
   local_48 = ZEXT816(0);
   if ((MmVerifierData & 0x10) != 0) {
     VfIoInitializeIrp(0,unaff_retaddr,1);
     IovpLogStackTrace(param_1);
   }
   bVar2 = *(byte *)((longlong)param_1 + 0x47);
   cVar7 = *(char *)(param_1 + 0x21);
   uVar4 = param_1[1];
   if ((char)*(byte *)((longlong)param_1 + 0x47) < '\0') {
     *(undefined8 *)(param_1 + 100) = 0;
     *(byte *)((longlong)param_1 + 0x47) = *(byte *)((longlong)param_1 + 0x47) & 0x7f;
   }
   else {
     if ((*(longlong *)(param_1 + 100) == 0) ||
        ((*(byte *)(*(longlong *)(param_1 + 100) + 2) & 1) == 0)) {
       lVar8 = *(longlong *)(param_1 + 100);
       bVar6 = false;
     }
     else {
       lVar8 = *(longlong *)(param_1 + 100);
       local_48 = *(undefined (*) [16])(lVar8 + 0x18);
       bVar6 = true;
     }
     if (lVar8 != 0) {
       if ((-1 < *(char *)((longlong)param_1 + 0x47)) && ((*(byte *)(lVar8 + 2) & 0x20) != 0)) {
         *(undefined8 *)(lVar8 + 0x28) = 0;
       }
-      if (((-1 < *(char *)((longlong)param_1 + 0x47)) && (*(longlong *)(param_1 + 100) != 0)) &&
-         ((*(ushort *)(*(longlong *)(param_1 + 100) + 2) >> 9 & 1) != 0)) {
-        if ((*(uint *)(param_1 + 8) >> 9 & 1) != 0) {
-          IopFreeCopyObjectsFromIrp(param_1);
-          *(undefined *)((longlong)param_1 + 0x41) = 1;
-          *(undefined2 *)(lVar8 + 2) = 0;
-          goto LAB_0;
-        }
-        if ((*(uint *)(param_1 + 8) >> 8 & 1) != 0) {
-          Feature_Servicing_CopyCancel_40135345__private_IsEnabled();
-        }
+      if ((((-1 < *(char *)((longlong)param_1 + 0x47)) && (*(longlong *)(param_1 + 100) != 0)) &&
+         ((*(ushort *)(*(longlong *)(param_1 + 100) + 2) >> 9 & 1) != 0)) &&
+         ((*(uint *)(param_1 + 8) >> 9 & 1) != 0)) {
+        IopFreeCopyObjectsFromIrp(param_1);
+        *(undefined *)((longlong)param_1 + 0x41) = 1;
       }
       *(undefined2 *)(lVar8 + 2) = 0;
     }
   }
```

```
-       if (((-1 < *(char *)((longlong)param_1 + 0x47)) && (*(longlong *)(param_1 + 100
-          ((*(ushort *)(*(longlong *)(param_1 + 100) + 2) >> 9 & 1) != 0)) {
-         if ((*(uint *)(param_1 + 8) >> 9 & 1) != 0) {
-           IopFreeCopyObjectsFromIrp(param_1);
-           *(undefined *)((longlong)param_1 + 0x41) = 1;
-           *(undefined2 *)(lVar8 + 2) = 0;
-           goto LAB_0;
-         }
-         if ((*(uint *)(param_1 + 8) >> 8 & 1) != 0) {
-           Feature_Servicing_CopyCancel_40135345__private_IsEnabled();
-         }
+       if ((((-1 < *(char *)((longlong)param_1 + 0x47)) && (*(longlong *)(param_1 + 10
+           ((*(ushort *)(*(longlong *)(param_1 + 100) + 2) >> 9 & 1) != 0)) &&
+          ((*(uint *)(param_1 + 8) >> 9 & 1) != 0)) {
+         IopFreeCopyObjectsFromIrp(param_1);
+         *(undefined *)((longlong)param_1 + 0x41) = 1;
        }
       *(undefined2 *)(lVar8 + 2) = 0;
     }
```

One Issue with Side by Side Diffs

ghidriff [Dev Container: ghidriff @ desktop-linux]

Preview ntoskrnl.exe.x64.10.0.22621.1105-ntoskrnl.exe.x64.10.0.22621.1194_diff.md

NtCreateLowBoxToken Side By Side Diff

ntoskrnl.exe.x64.10.0.22621.1105

```
/* WARNING: Globals starting with '_' overlap smaller symbols at the same address */

ulonglong NtCreateLowBoxToken(longlong *param_1,undefined8 param_2,int param_3,undefined8 param_4,
                              longlong param_5,uint param_6,longlong param_7,uint param_8,
                              ulonglong param_9)

{
  char cVar1;
  byte bVar2;
  undefined8 uVar3;
  bool bVar4;
  bool bVar5;
  bool bVar6;

  char cVar7;
  uint uVar8;
  int iVar9;
  longlong *plVar10;
  undefined4 *puVar11;
```

ntoskrnl.exe.x64.10.0.22621.1194

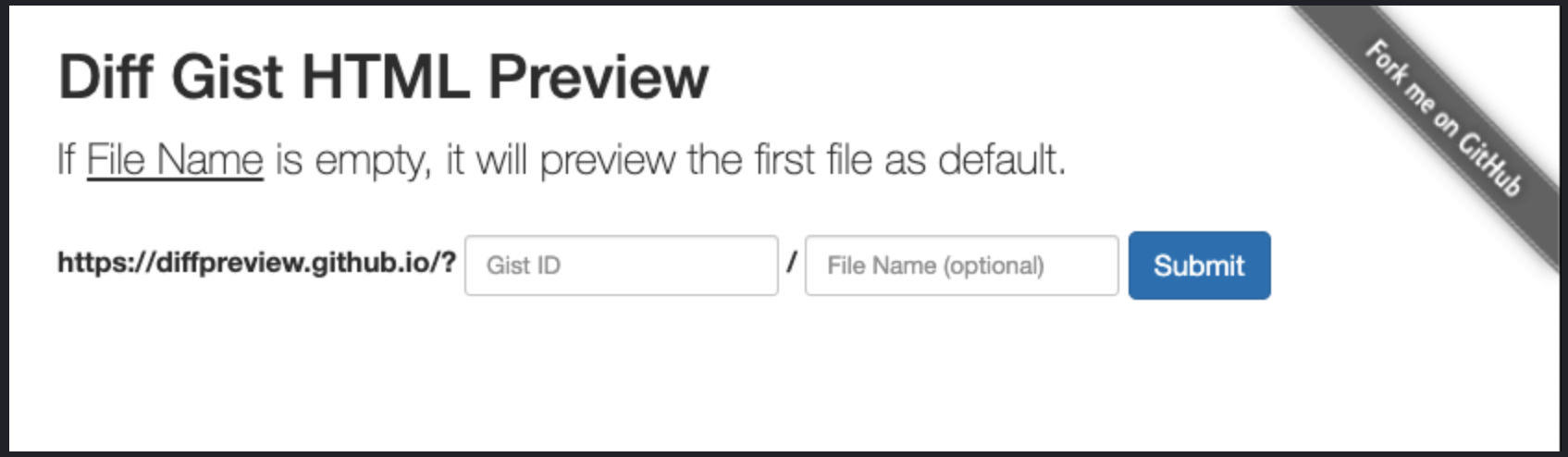
```
/* WARNING: Globals starting with '_' overlap smaller symbols at the same address */

ulonglong NtCreateLowBoxToken(longlong *param_1,undefined8 param_2,int param_3,undefine
                              longlong param_5,uint param_6,longlong param_7,uint param_
                              ulonglong param_9)

{
  char cVar1;
  byte bVar2;
  undefined8 uVar3;
  int iVar4;
  bool bVar5;
  bool bVar6;
  bool bVar7;
  char cVar8;
  uint uVar9;

  longlong *plVar10;
  undefined4 *puVar11;
```

Markdown in GitHub / GitLab won't render HTML style

IoReuseIrp Side By Side Diff

<style type="text/css"> table.diff {font-family:Courier; border:medium;} .diff_header {background-color:#e0e0e0} td.diff_header {text-align:right} .diff_next {background-color:#c0c0c0} .diff_add {background-color:#aaffaa} .diff_chg {background-color:#ffff77} .diff_sub {background-color:#ffaaaa} </style>

ntoskrnl.exe.x64.10.0.22621.1105			
	f	1	
void IoReuseIrp(undefined2 *param_1,undefined4 param_2)		2	void IoReuseI
		3	
{		4	{
undefined2 *puVar1;		5	undefined2 *
byte bVar2;		6	byte bVar2;
undefined uVar3;		7	undefined uV
ushort uVar4;		8	ushort uVar4
undefined2 uVar5;		9	undefined2 u
bool bVar6;		10	bool bVar6;



https://diffpreview.github.io/

https://gist.github.com/clearbluejar/fc20a4f6f2a9e91d5ed7104eedea53e0

https://diffpreview.github.io/?fc20a4f6f2a9e91d5ed7104eedea53e0

Diff Gist HTML Preview

If File Name is empty, it will preview the first file as default.

https://diffpreview.github.io/? fc20a4f6f2a9e91d5ed710 / File Name (optional) Submit

Fork me on GitHub

Gist Details:

- url : https://api.github.com/gists/fc20a4f6f2a9e91d5ed7104eedea53e0
- id : fc20a4f6f2a9e91d5ed7104eedea53e0
- description :

Files from Gist: 1

- ntoskrnl.exe.x64.10.0.22621.1105-ntoskrnl.exe.x64.10.0.22621.1194.diff.md (497 Bytes) [raw_gist]

Files changed (57) hide

ntoskrnl.exe.x64.10.0.22621.1105 Meta → ntoskrnl.exe.x64.10.0.22621.1194 Meta	+14	-14
Feature_Servicing_CopyCancel_40135345__private_IsEnabled	+0	-17
IopCopyCompleteIrp	+0	-85
Feature_Servicing_SRQueryRelations__private_IsEnabled	+0	-17
Feature_Servicing_EaseTokenSACLPPLRestrictions__private_IsEnabled	+0	-18
SepAppendAdminAceToTokenAcl	+0	-8
NtCreateLowBoxToken called	+0	-1
NtCreateLowBoxToken	+60	-66
IopfCompleteRequest called	+0	-2
IopfCompleteRequest	+0	-4
SeSubProcessToken called	+0	-3
SeSubProcessToken	+1	-8
IoReuseIrp called	+0	-1
IoReuseIrp	+8	-15

IoReuseIrp CHANGED

Viewed

```diff
@@ -1,112 +1,105 @@
 void IoReuseIrp(undefined2 *param_1,undefined4 param_2)
 {
   undefined2 *puVar1;
   byte bVar2;
   undefined uVar3;
   ushort uVar4;
   undefined2 uVar5;
   bool bVar6;
   char cVar7;
   longlong lVar8;
   undefined8 unaff_retaddr;
   undefined auStack_88 [32];
   longlong local_68;
   undefined *local_60;
   undefined4 local_58;
   undefined8 local_50;
   undefined local_48 [16];
   ulonglong local_38;
-                    /* 0x347500  1038  IoReuseIrp */
   local_38 = __security_cookie ^ (ulonglong)auStack_88;
   bVar6 = false;
   local_48 = ZEXT816(0);
   if ((MmVerifierData & 0x10) != 0) {
     VfIoInitializeIrp(0,unaff_retaddr,1);
     IovpLogStackTrace(param_1);
   }
   bVar2 = *(byte *)((longlong)param_1 + 0x47);
   cVar7 = *(char *)(param_1 + 0x21);
   uVar4 = param_1[1];
   if ((char)*(byte *)((longlong)param_1 + 0x47) < '\0') {
     *(undefined8 *)(param_1 + 100) = 0;
     *(byte *)((longlong)param_1 + 0x47) = *(byte *)((longlong)param_1 + 0x47) & 0x7f;
   }
   else {
     if ((*(longlong *)(param_1 + 100) == 0) ||
        ((*(byte *)(*(longlong *)(param_1 + 100) + 2) & 1) == 0)) {
       lVar8 = *(longlong *)(param_1 + 100);
       bVar6 = false;
     }
     else {
       lVar8 = *(longlong *)(param_1 + 100);
       local_48 = *(undefined (*) [16])(lVar8 + 0x18);
       bVar6 = true;
     }
     if (lVar8 != 0) {
       if ((-1 < *(char *)((longlong)param_1 + 0x47)) && ((*(byte *)(lVar8 + 2) & 0x20) !
         *(undefined8 *)(lVar8 + 0x28) = 0;
       }
-      if (((-1 < *(char *)((longlong)param_1 + 0x47)) && (*(longlong *)(param_1 + 100) !
-         ((*(ushort *)(*(longlong *)(param_1 + 100) + 2) >> 9 & 1) != 0)) {
-        if ((*(uint *)(param_1 + 8) >> 9 & 1) != 0) {
-          IopFreeCopyObjectsFromIrp(param_1);
-          *(undefined *)((longlong)param_1 + 0x41) = 1;
-          *(undefined2 *)(lVar8 + 2) = 0;
-          goto LAB_0;
-        }
-        if ((*(uint *)(param_1 + 8) >> 8 & 1) != 0) {
-          Feature_Servicing_CopyCancel_40135345__private_IsEnabled();
-        }
       }
       *(undefined2 *)(lVar8 + 2) = 0;
     }
   }
```

```diff
 void IoReuseIrp(undefined2 *param_1,undefined4 param_2)
 {
   undefined2 *puVar1;
   byte bVar2;
   undefined uVar3;
   ushort uVar4;
   undefined2 uVar5;
   bool bVar6;
   char cVar7;
   longlong lVar8;
   undefined8 unaff_retaddr;
   undefined auStack_88 [32];
   longlong local_68;
   undefined *local_60;
   undefined4 local_58;
   undefined8 local_50;
   undefined local_48 [16];
   ulonglong local_38;
+                    /* 0x3473c0  1038  IoReuseIrp */
   local_38 = __security_cookie ^ (ulonglong)auStack_88;
   bVar6 = false;
   local_48 = ZEXT816(0);
   if ((MmVerifierData & 0x10) != 0) {
     VfIoInitializeIrp(0,unaff_retaddr,1);
     IovpLogStackTrace(param_1);
   }
   bVar2 = *(byte *)((longlong)param_1 + 0x47);
   cVar7 = *(char *)(param_1 + 0x21);
   uVar4 = param_1[1];
   if ((char)*(byte *)((longlong)param_1 + 0x47) < '\0') {
     *(undefined8 *)(param_1 + 100) = 0;
     *(byte *)((longlong)param_1 + 0x47) = *(byte *)((longlong)param_1 + 0x47) & 0x7f;
   }
   else {
     if ((*(longlong *)(param_1 + 100) == 0) ||
        ((*(byte *)(*(longlong *)(param_1 + 100) + 2) & 1) == 0)) {
       lVar8 = *(longlong *)(param_1 + 100);
       bVar6 = false;
     }
     else {
       lVar8 = *(longlong *)(param_1 + 100);
       local_48 = *(undefined (*) [16])(lVar8 + 0x18);
       bVar6 = true;
     }
     if (lVar8 != 0) {
       if ((-1 < *(char *)((longlong)param_1 + 0x47)) && ((*(byte *)(lVar8 + 2) & 0x20) !
         *(undefined8 *)(lVar8 + 0x28) = 0;
       }
+      if ((((-1 < *(char *)((longlong)param_1 + 0x47)) && (*(longlong *)(param_1 + 100)
+         ((*(ushort *)(*(longlong *)(param_1 + 100) + 2) >> 9 & 1) != 0)) &&
+         ((*(uint *)(param_1 + 8) >> 9 & 1) != 0)) {
+        IopFreeCopyObjectsFromIrp(param_1);
+        *(undefined *)((longlong)param_1 + 0x41) = 1;
       }
       *(undefined2 *)(lVar8 + 2) = 0;
     }
   }
```

IoReuseIrp CHANGED

Viewed

```
48        }
49 -      if (((-1 < *(char *)((longlong)param_1 + 0x47)) && (*
50 -         ((*(ushort *)(*(longlong *)(param_1 + 100) + 2) >>
51 -        if ((*(uint *)(param_1 + 8) >> 9 & 1) != 0) {
52 -          IopFreeCopyObjectsFromIrp(param_1);
53 -          *(undefined *)((longlong)param_1 + 0x41) = 1;
54 -          *(undefined2 *)(lVar8 + 2) = 0;
55 -          goto LAB_0;
56 -        }
57 -        if ((*(uint *)(param_1 + 8) >> 8 & 1) != 0) {
58 -          Feature_Servicing_CopyCancel_40135345__private_Is
59 -        }
60        }
61        *(undefined2 *)(lVar8 + 2) = 0;
62      }
63    }
```

```
48        }
49 +      if ((((-1 < *(char *)((longlong)param_1 + 0x47)) && (
50 +         ((*(ushort *)(*(longlong *)(param_1 + 100) + 2) >
51 +         ((*(uint *)(param_1 + 8) >> 9 & 1) != 0)) {
52 +        IopFreeCopyObjectsFromIrp(param_1);
53 +        *(undefined *)((longlong)param_1 + 0x41) = 1;
54        }
55        *(undefined2 *)(lVar8 + 2) = 0;
56      }
57    }
```

Ghidriff in Action

```
ghidriff ntoskrnl.exe.x64.10.0.22621.1105
    ntoskrnl.exe.x64.10.0.22621.1194
```

Sample Log Output

```
(.env) vscode ➜ /workspaces/ghidriff (main) $ ghidriff bins/ntoskrnl.exe.x64.10.0.22621.1105 bins/ntoskrnl.exe.x64.10.0.22621.1194
INFO | ghidriff | Init Ghidra Diff Engine...
INFO | ghidriff | Engine Console Log: INFO
INFO | ghidriff | Engine File Log:  ghidriffs/ghidriff.log INFO
INFO | ghidriff | Starting Ghidra...
INFO  Using log config file: jar:file:/ghidra/Ghidra/Framework/Generic/lib/Generic.jar!/generic.log4j.xml (LoggingInitialization)
INFO  Using log file: /workspaces/ghidriff/ghidriffs/ghidriff.log (LoggingInitialization)
INFO  Loading user preferences: /home/vscode/.ghidra/.ghidra_10.3.3_PUBLIC/preferences (Preferences)
INFO  Searching for classes... (ClassSearcher)
INFO  Class search complete (756 ms) (ClassSearcher)
INFO  Initializing SSL Context (SSLContextInitializer)
INFO  Initializing Random Number Generator... (SecureRandomFactory)
INFO  Random Number Generator initialization complete: NativePRNGNonBlocking (SecureRandomFactory)
INFO  Trust manager disabled, cacerts have not been set (ApplicationTrustManagerFactory)
INFO | ghidriff | GHIDRA_INSTALL_DIR: /ghidra
INFO | ghidriff | GHIDRA 10.3.3  Build Date: 2023-Aug-29 1442 EDT Release: PUBLIC
INFO | ghidriff | Engine Args:
INFO | ghidriff |       old:                ['bins/ntoskrnl.exe.x64.10.0.22621.1105']
INFO | ghidriff |       new:                [['bins/ntoskrnl.exe.x64.10.0.22621.1194']]
INFO | ghidriff |       engine:             VersionTrackingDiff
INFO | ghidriff |       output_path:        ghidriffs
INFO | ghidriff |       summary:            False
INFO | ghidriff |       project_location:   .ghidra_projects
INFO | ghidriff |       project_name:       ghidriff
INFO | ghidriff |       symbols_path:       .symbols
INFO | ghidriff |       threaded:           True
INFO | ghidriff |       force_analysis:     False
INFO | ghidriff |       force_diff:         False
INFO | ghidriff |       no_symbols:         False
INFO | ghidriff |       log_level:          INFO
INFO | ghidriff |       file_log_level:     INFO
INFO | ghidriff |       log_path:           ghidriff.log
INFO | ghidriff |       va:                 False
INFO | ghidriff |       max_ram_percent:    60.0
```

```
INFO | ghidriff | Setting Up Ghidra Project...
INFO  Opening project: /workspaces/ghidriff/.ghidra_projects/ghidriff-ntoskrnl.exe.x64.10.0.22621.1105-ntoskrnl.exe.x64.10.0.22621.1194/ghid
riff-ntoskrnl.exe.x64.10.0.22621.1105-ntoskrnl.exe.x64.10.0.22621.1194 (DefaultProject)
INFO | ghidriff | Opened project: ghidriff-ntoskrnl.exe.x64.10.0.22621.1105-ntoskrnl.exe.x64.10.0.22621.1194
INFO | ghidriff | Project Location: /workspaces/ghidriff/.ghidra_projects/ghidriff-ntoskrnl.exe.x64.10.0.22621.1105-ntoskrnl.exe.x64.10.0.22
621.1194
INFO | ghidriff | Opening bins/ntoskrnl.exe.x64.10.0.22621.1105
INFO | ghidriff | Opening bins/ntoskrnl.exe.x64.10.0.22621.1194
INFO | ghidriff | Setting up Symbol Server for symbols...
INFO | ghidriff | path: .symbols level: 1
INFO | ghidriff | Symbol Server Configured path: SymbolServerService:
        symbolStore: LocalSymbolStore: [ rootDir: /workspaces/ghidriff/.symbols, storageLevel: -1],
        symbolServers:
                HttpSymbolServer: [ url: https://msdl.microsoft.com/download/symbols/, storageLevel: -1]
                HttpSymbolServer: [ url: https://chromium-browser-symsrv.commondatastorage.googleapis.com/, storageLevel: -1]
                HttpSymbolServer: [ url: https://symbols.mozilla.org/, storageLevel: -1]
                HttpSymbolServer: [ url: https://software.intel.com/sites/downloads/symbols/, storageLevel: -1]
                HttpSymbolServer: [ url: https://driver-symbols.nvidia.com/, storageLevel: -1]
                HttpSymbolServer: [ url: https://download.amd.com/dir/bin/, storageLevel: -1]
INFO | ghidriff | Pdb stored at: /workspaces/ghidriff/.symbols/ntkrnlmp.pdb/4738AC02284CCC451E86A727E513D1131/ntkrnlmp.pdb
INFO | ghidriff | Pdb stored at: /workspaces/ghidriff/.symbols/ntkrnlmp.pdb/8F0F3D677778391600F4EB2301FFC7A51/ntkrnlmp.pdb
INFO | ghidriff | Program: /workspaces/ghidriff/bins/ntoskrnl.exe.x64.10.0.22621.1105 imported: True has_pdb: True pdb_loaded: True analyzed
 True
INFO | ghidriff | Program: /workspaces/ghidriff/bins/ntoskrnl.exe.x64.10.0.22621.1194 imported: True has_pdb: True pdb_loaded: True analyzed
 True
INFO | ghidriff | Starting analysis for 2 binaries
INFO | ghidriff | Analyzing: ntoskrnl.exe.x64.10.0.22621.1194 - .ProgramDB
INFO | ghidriff | Analysis already complete.. skipping ntoskrnl.exe.x64.10.0.22621.1194 - .ProgramDB!
INFO | ghidriff | Analysis for ghidriff-ntoskrnl.exe.x64.10.0.22621.1105-ntoskrnl.exe.x64.10.0.22621.1194:/ntoskrnl.exe.x64.10.0.22621.1194-
951a21 complete
INFO | ghidriff | Analyzing: ntoskrnl.exe.x64.10.0.22621.1105 - .ProgramDB
INFO | ghidriff | Analysis already complete.. skipping ntoskrnl.exe.x64.10.0.22621.1105 - .ProgramDB!
INFO | ghidriff | Analysis for ghidriff-ntoskrnl.exe.x64.10.0.22621.1105-ntoskrnl.exe.x64.10.0.22621.1194:/ntoskrnl.exe.x64.10.0.22621.1105-
```

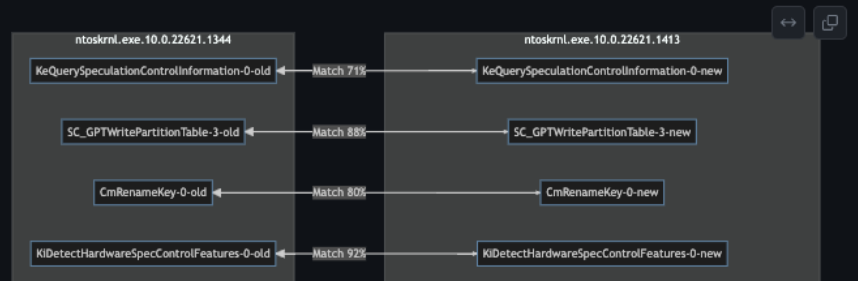
```
INFO | ghidriff | Diffing bins: bins/ntoskrnl.exe.x64.10.0.22621.1105 - bins/ntoskrnl.exe.x64.10.0.22621.1194
INFO | ghidriff | Setup 16 decompliers
INFO | ghidriff | Loaded old program: ntoskrnl.exe.x64.10.0.22621.1105
INFO | ghidriff | Loaded new program: ntoskrnl.exe.x64.10.0.22621.1194
INFO | ghidriff | p1 sym count: reported: 245738 analyzed: 16857
INFO | ghidriff | p2 sym count: reported: 245722 analyzed: 16848
INFO | ghidriff | Found unmatched: 37 matched: 16834 symbols
INFO  Hashing symbols in ntoskrnl.exe.x64.10.0.22621.1105 (ConsoleTaskMonitor)
INFO  Hashing symbols in ntoskrnl.exe.x64.10.0.22621.1194 (ConsoleTaskMonitor)
INFO  Eliminate non-unique matches (ConsoleTaskMonitor)
INFO  Finding symbol matches (ConsoleTaskMonitor)
INFO | ghidriff | Exec time: 1.4149 secs
INFO | ghidriff | Match count 54956
INFO | ghidriff | Counter({('SymbolsHash',): 27913})
INFO | ghidriff | Running correlator: ExactBytesFunctionHasher
INFO | ghidriff | name: ExactBytesFunctionHasher one_to_one: True one_to_many: False
INFO  Hashing functions in ntoskrnl.exe.x64.10.0.22621.1105 (ConsoleTaskMonitor)
INFO  Hashing functions in ntoskrnl.exe.x64.10.0.22621.1194 (ConsoleTaskMonitor)
INFO  Finding function matches (ConsoleTaskMonitor)
INFO | ghidriff | ExactBytesFunctionHasher Exec time: 0.8368 secs
INFO | ghidriff | Match count: 79
INFO | ghidriff | Running correlator: ExactInstructionsFunctionHasher
INFO | ghidriff | name: ExactInstructionsFunctionHasher one_to_one: True one_to_many: False
INFO | ghidriff | ExactInstructionsFunctionHasher Exec time: 0.4648 secs
INFO | ghidriff | Match count: 138
INFO | ghidriff | Running correlator: StructuralGraphExactHash
INFO | ghidriff | name: StructuralGraphExactHash one_to_one: True one_to_many: False
INFO | ghidriff | StructuralGraphExactHash Exec time: 0.5948 secs
INFO | ghidriff | Match count: 0
INFO | ghidriff | Running correlator: ExactMnemonicsFunctionHasher
INFO | ghidriff | name: ExactMnemonicsFunctionHasher one_to_one: True one_to_many: False
INFO | ghidriff | ExactMnemonicsFunctionHasher Exec time: 0.2371 secs
INFO | ghidriff | Match count: 0
INFO | ghidriff | Running correlator: BulkInstructionHash
```

```
INFO | ghidriff | p1 missing = 5
INFO | ghidriff | p2 missing = 0
INFO | ghidriff | Deduping symbols and functions...
INFO | ghidriff | Sorting symbols and strings...
INFO | ghidriff | Sorting functions...
INFO | ghidriff | Starting esym lookups for 82 symbols using 8 threads
INFO | ghidriff | Completed 5 at 6%
INFO | ghidriff | Completed 10 at 12%
INFO | ghidriff | Completed 15 at 18%
INFO | ghidriff | Completed 20 at 24%
INFO | ghidriff | Completed 25 at 30%
INFO | ghidriff | Completed 30 at 36%
INFO | ghidriff | Completed 35 at 42%
INFO | ghidriff | Completed 40 at 48%
INFO | ghidriff | Completed 45 at 54%
INFO | ghidriff | Completed 50 at 60%
INFO | ghidriff | Completed 55 at 67%
INFO | ghidriff | Completed 60 at 73%
INFO | ghidriff | Completed 65 at 79%
INFO | ghidriff | Completed 70 at 85%
INFO | ghidriff | Completed 75 at 91%
INFO | ghidriff | Completed 80 at 97%
WARNING| ghidriff | Code diff type not appended for XpressBuildHuffmanDecodingTable due to jumptable decomp issue
INFO | ghidriff | Finished diffing old program: ntoskrnl.exe.x64.10.0.22621.1105
INFO | ghidriff | Finished diffing program: ntoskrnl.exe.x64.10.0.22621.1194
INFO | ghidriff | Writing md diff...
INFO | ghidriff | Generating markdown from {'added_funcs_len': 0, 'deleted_funcs_len': 5, 'modified_funcs_len': 36, 'added_symbols_len': 14, 'deleted_symbols_len': 23,
 'diff_time': 71.9299750328064, 'deleted_strings_len': 0, 'added_strings_len': 0, 'match_types': Counter({'SymbolsHash': 27913, 'StructuralGraphHash': 695, 'ExactInstr
uctionsFunctionHasher': 138, 'ExactBytesFunctionHasher': 79, 'BulkBasicBlockMnemonicHash': 2}), 'items_to_process': 78, 'diff_types': Counter({'address': 33, 'refcount
': 25, 'length': 20, 'code': 19, 'called': 17, 'calling': 15, 'sig': 1}), 'unmatched_funcs_len': 5, 'total_funcs_len': 60696, 'matched_funcs_len': 60691, 'matched_func
s_with_code_changes_len': 19, 'matched_funcs_with_non_code_changes_len': 17, 'matched_funcs_no_changes_len': 60655, 'match_func_similarity_percent': '99.9407%', 'func_
match_overall_percent': '99.9918%'}
INFO | ghidriff | Known Command line: python ghidriff --project-location .ghidra_projects --project-name ghidriff --symbols-path .symbols --threaded --log-level INFO -
-file-log-level INFO --log-path ghidriff.log --max-ram-percent 60.0 --max-section-funcs 200 ntoskrnl.exe.x64.10.0.22621.1105 ntoskrnl.exe.x64.10.0.22621.1194
INFO | ghidriff | Extra Command line: --engine VersionTrackingDiff --output-path ghidriffs
INFO | ghidriff | Writing pdiff json...
INFO | ghidriff | Wrote ghidriffs/ntoskrnl.exe.x64.10.0.22621.1105-ntoskrnl.exe.x64.10.0.22621.1194_diff.md
INFO | ghidriff | Wrote ghidriffs/json/ntoskrnl.exe.x64.10.0.22621.1105-ntoskrnl.exe.x64.10.0.22621.1194_diff.json
```

ntoskrnl.exe.10.0.22621.1344-ntoskrnl.exe.10.0.22621.1413 Diff

TOC

Visual Chart Diff



CVE Diffs

CVE-2023-21768

Security Intelligence

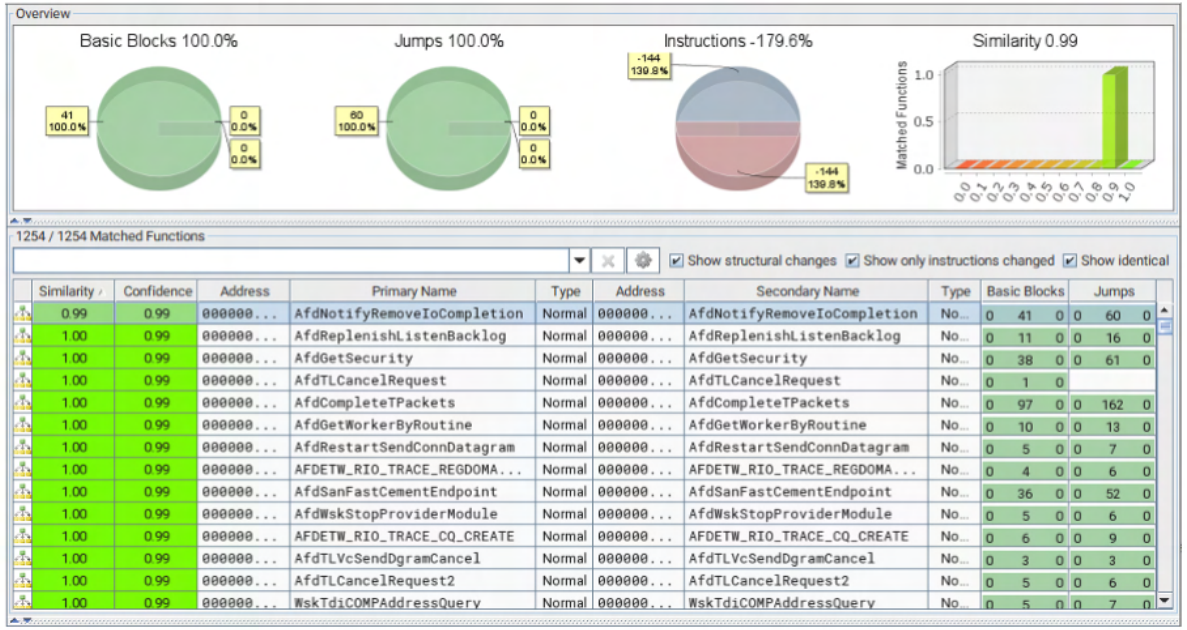
Patch Tuesday -> exploit Wednesday: Pwning windows ancillary function driver for WinSock (afd.sys) in 24 hours

Adversary Services | March 21, 2023

By Valentina Palmiotti, Ruben Boonen | 12 min read

Series: Offensive Research

Ghidra was used to create binary exports for both of these files so they could be compared in BinDiff. An overview of the matched functions is shown below.



Similarity	Confidence	Address	Primary Name	Type	Address	Secondary Name	Type	Basic Blocks	Jumps
0.99	0.99	000000...	AfdNotifyRemoveIoCompletion	Normal	000000...	AfdNotifyRemoveIoCompletion	No...	0 41 0	0 60 0
1.00	0.99	000000...	AfdReplenishListenBacklog	Normal	000000...	AfdReplenishListenBacklog	No...	0 11 0	0 16 0
1.00	0.99	000000...	AfdGetSecurity	Normal	000000...	AfdGetSecurity	No...	0 38 0	0 61 0
1.00	0.99	000000...	AfdTLCancelRequest	Normal	000000...	AfdTLCancelRequest	No...	0 1 0	
1.00	0.99	000000...	AfdCompleteTPackets	Normal	000000...	AfdCompleteTPackets	No...	0 97 0	0 162 0
1.00	0.99	000000...	AfdGetWorkerByRoutine	Normal	000000...	AfdGetWorkerByRoutine	No...	0 10 0	0 13 0
1.00	0.99	000000...	AfdRestartSendConnDatagram	Normal	000000...	AfdRestartSendConnDatagram	No...	0 5 0	0 7 0
1.00	0.99	000000...	AFDETW_RIO_TRACE_REGDOMA...	Normal	000000...	AFDETW_RIO_TRACE_REGDOMA...	No...	0 4 0	0 6 0
1.00	0.99	000000...	AfdSanFastCementEndpoint	Normal	000000...	AfdSanFastCementEndpoint	No...	0 36 0	0 52 0
1.00	0.99	000000...	AfdWskStopProviderModule	Normal	000000...	AfdWskStopProviderModule	No...	0 5 0	0 6 0
1.00	0.99	000000...	AFDETW_RIO_TRACE_CQ_CREATE	Normal	000000...	AFDETW_RIO_TRACE_CQ_CREATE	No...	0 6 0	0 9 0
1.00	0.99	000000...	AfdTLVcSendDgramCancel	Normal	000000...	AfdTLVcSendDgramCancel	No...	0 3 0	0 3 0
1.00	0.99	000000...	AfdTLCancelRequest2	Normal	000000...	AfdTLCancelRequest2	No...	0 5 0	0 6 0
1.00	0.99	000000...	WskTdiCOMPAddressQuery	Normal	000000...	WskTdiCOMPAddressQuery	No...	0 5 0	0 7 0

Missing user mode buffer check in

`afd!AfdNotifyRemoveIoCompletion`

1. Download `afd.sys` (vulnerable and patched):

```
wget https://msdl.microsoft.com/download/symbols/afd.sys/0C5C6994A8000/afd.sys -O afd.sys.x64.10.0.22621.1028
wget https://msdl.microsoft.com/download/symbols/afd.sys/50989142A9000/afd.sys -O afd.sys.x64.10.0.22621.1415
```

2. Run `ghidriff`:

```
ghidriff afd.sys.x64.10.0.22621.1028 afd.sys.x64.10.0.22621.1415
```

3. Analyze Diff

- Deleted
- Added
  - wil_details_FeatureDescriptors_SkipPadding
  - Feature_Servicing_SiloCrashFixinAFD__private_IsEnabled
  - wil_details_FeatureReporting_IncrementOpportunityInCache
  - wil_details_FeatureReporting_IncrementUsageInCache
  - wil_details_FeatureReporting_RecordUsageInCache
  - NTOSKRNL.EXE::RtlNotifyFeatureUsage
  - NTOSKRNL.EXE::RtlUnregisterFeatureConfigurationChangeNotification
  - NTOSKRNL.EXE::RtlQueryFeatureConfigurationChangeStamp
- Modified
  - DriverEntry
  - AfdNsiAddressChangeEventAtPassive
  - AfdUnload
  - AfdNotifyRemoveIoCompletion
- Modified (No Code Changes)
  - __GSHandlerCheck
  - _guard_dispatch_icall
  - AfdAllocateBuffer
  - FastWppCallback
  - AfdPodGetCurrent
  - __security_check_cookie

```
  iVar3 = IoRemoveIoCompletion(local_2e0,puVar5,puVar6,uVar11);
  if (iVar3 == 0) {
    if (local_307 != '\0') {
      for (uVar9 = 0; uVar9 < local_304; uVar9 = uVar9 + 1) {
        puVar8 = (undefined4 *)(puVar5 + (ulonglong)uVar9 * 0x20);
        puVar7 = (undefined4 *)((ulonglong)uVar9 * 0x10 + *(longlong *)(param_3 + 0x10));
        *puVar7 = *puVar8;
        puVar7[1] = puVar8[2];
        puVar7[3] = puVar8[6];
        puVar7[2] = puVar8[4];
      }
    }
    if (cVar2 == '\0') {
      **(uint **)(param_3 + 0x18) = local_304;
    }
    else {
+     ProbeForWrite(*(undefined8 *)(param_3 + 0x18),4,4);
      **(uint **)(param_3 + 0x18) = local_304;
    }
  }
```

CVE-2023-21769

QUEUEJUMPER: CRITICAL UNAUTHENTICATED RCE VULNERABILITY IN MSMQ SERVICE

April 11, 2023

Research by: Haifei Li.

msmq_re

This is one of the vulnerabilities fixed in MSMQ.

> https://research.checkpoint.com/2023/queuejumper-critical-unauthorized-rce-vulnerability-in-msmq-service/

```
0:064> r
rax=0000000000001000 rbx=000001b4ee9b5cf8 rcx=000000000000006
rdx=000001b4240b5c24 rsi=000000000000002 rdi=00000008e6c7fb10
rip=00007ffcc9708b80 rsp=00000008e6c7fa00 rbp=00000008e6c7fa40
 r8=0000000000000000  r9=000001b4247e3d90 r10=000001b4240b5c34
r11=00000008e6c7f9f8 r12=000000000000000 r13=000000000000001
r14=0000000000000001 r15=000001b4240b5dec
iopl=0         nv up ei pl zr na po nc
cs=0033  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010244
MQQM!CQmPacket::CQmPacket+0x8fc:
00007ffc`c9708b80 48c7030c000000  mov     qword ptr [rbx],0Ch ds:000001b4`ee9b5cf8=????????????????
0:064> k
 # Child-SP          RetAddr               Call Site
00 00000008`e6c7fa00 00007ffc`c972699a     MQQM!CQmPacket::CQmPacket+0x8fc
01 00000008`e6c7fa70 00007ffc`c9723836     MQQM!CSockTransport::HandleReceiveUserMsg+0x62
02 00000008`e6c7fcd0 00007ffc`c9723bd2     MQQM!CSockTransport::ReadUserMsgCompleted+0xd6
03 00000008`e6c7fd30 00007ffc`c9723faf     MQQM!CSockTransport::ReadUsrHeaderCompleted+0x312
04 00000008`e6c7fde0 00007ffc`c9723eac     MQQM!CSockTransport::ReadCompleted+0xef
05 00000008`e6c7fe40 00007ffc`c976ea2a     MQQM!CSockTransport::ReceiveDataSucceeded+0x7c
06 00000008`e6c7fe80 00007ffc`d2334de0     MQQM!ExpWorkingThread+0xfa
07 00000008`e6c7fed0 00007ffc`d2ffe3db     KERNEL32!BaseThreadInitThunk+0x10
08 00000008`e6c7ff00 00000000`00000000     ntdll!RtlUserThreadStart+0x2b
```

msmq_re

Packet parsing code in function `CQmPacket::CQmPacket` within `mqqm.dll` has the issue...

1. Download `mqqm.dll` (vulnerable and patched):

```
wget https://msdl.microsoft.com/download/symbols/afd.sys/0C5C6994A8000/afd.sys -O afd.sys.x64.10.0.22621.1028
wget https://msdl.microsoft.com/download/symbols/afd.sys/50989142A9000/afd.sys -O afd.sys.x64.10.0.22621.1415
```

2. Run `ghidriff`:

```
ghidriff afd.sys.x64.10.0.22621.1028 afd.sys.x64.10.0.22621.1415
```

- Modified
  - CUserHeader::SectionIsValid
  - CDebugSection::SectionIsValid
  - CBaseMqfHeader::SectionIsValid
  - CXactHeader::SectionIsValid
  - wil::details::`dynamic_initializer_for_'g_header_init_InitializeStagingHeaderInternalApi''
  - wil::details::StringCchPrintfA
  - CPropertyHeader::SectionIsValid
  - CQmPacket::CQmPacket
  - CMsgDeadletterHeader::SectionIsValid
  - CUserHeader::QueueSize
  - CMsgGroupHeader::SectionIsValid
  - StringCchVPrintfW
  - StringCchCopyA
  - CSecurityHeader::SectionIsValid

CQmPacket::CQmPacket Called Diff

```diff
--- CQmPacket::CQmPacket called
+++ CQmPacket::CQmPacket called
@@ -7,0 +8 @@
+CEodHeader::GetNextSectionSafe
@@ -9,0 +11 @@
+CMqfSignatureHeader::SectionIsValid
@@ -19,0 +22 @@
+CSoapSection::GetNextSectionSafe
@@ -24,2 +27 @@
-LogIllegalPoint
-MSVCRT.DLL::exception::exception
+GetNextSectionPtrSafe
@@ -28,2 +29,0 @@
-WPP_SF_
-_CxxThrowException
@@ -30,0 +31 @@
+wil::details::FeatureImpl<struct___WilFeatureTraits_Feature_MSRC76146_MSMQ_OOBRWFixes>
```

CQmPacket::CQmPacket CHANGED

Viewed

```
153 -       if (param_3) {
154 -         pCVar11 = (CBaseHeader *)CMqfSignatureHeader::GetNext
155 -         if (pCVar15 < pCVar11) {
156 -           if (((undefined **)WPP_GLOBAL_Control != &WPP_GLOBA
157 -               ((WPP_GLOBAL_Control[0x6c] & 1) != 0)) {
158 -             WPP_SF_(*(undefined8 *)(WPP_GLOBAL_Control + 0x60
159 -                   &WPP_a42e52f147c9336096d5a05ce72d54ca_Tra
160 -           }
161 -           LogIllegalPoint((wchar_t *)L"verifypacket",0x5fb);
162 -           exception::exception((exception *)&local_48);
163 -                   /* WARNING: Subroutine does not return */
164 -           _CxxThrowException(&local_48,(ThrowInfo *)&_TI1_AVe
165         }
166 -       }
167 -       puVar8 = (undefined8 *)
168 -               CMqfSignatureHeader::GetNextSection(*(CMqfSigr
169 -     }
170 -     lVar14 = *(longlong *)(this + 0x30);
```

```
161 +       if (param_3) {
162 +         CMqfSignatureHeader::SectionIsValid(this_06,(char *)p
163 +       }
164 +       this_05 = (undefined8 *)
165 +               CMqfSignatureHeader::GetNextSection(*(CMqfSig
166 +     }
167 +     if ((*(uint *)(*(longlong *)(this + 0x30) + 0x2c) & 0x200
168 +       puVar3 = *(undefined8 **)(this + 0x28);
169 +       if ((undefined8 *)((ulonglong)*(uint *)(puVar3 + 1) + (
170 +       goto LAB_0;
171 +       if (this_05 < puVar3) goto LAB_1;
172 +       *(undefined8 **)(this + 0x78) = this_05;
173 +       bVar11 = wil::details::
174 +               FeatureImpl<struct___WilFeatureTraits_Feature_
175 +               __private_IsEnabled(&`private:_static_class_wi
176 +                                   ::`2'::impl);
177 +       _Var6 = *(__uint64 *)(this + 0x78);
178 +       if ((bVar11) && (param_3)) {
179 +         uVar10 = (ulonglong)*(uint *)(_Var6 + 4) * 2;
180 +         if (0xffffffff < uVar10) {
181 +           ReportAndThrow("DataLength caused overflow");
182 +           pcVar9 = (code *)swi(3);
183 +           pCVar18 = (CQmPacket *)(*pcVar9)();
184 +           return pCVar18;
185         }
186 +       pcVar14 = GetNextSectionPtrSafe(_Var6,8,uVar10 & 0xff
187 +       }
188 +       else {
189 +         pcVar14 = (char *)(((ulonglong)(*(int *)(_Var6 + 4) *
190 +       }
```

Root Cause Your Own CVEs

CVE-2023-36903

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36903

- Published last month
- No known blogs or pocs

MSRC > Customer Guidance > Security Update Guide > Vulnerabilities > CVE 2023 36903

Windows System Assessment Tool Elevation of Privilege Vulnerability

CVE-2023-36903
Security Vulnerability

Released: Aug 8, 2023

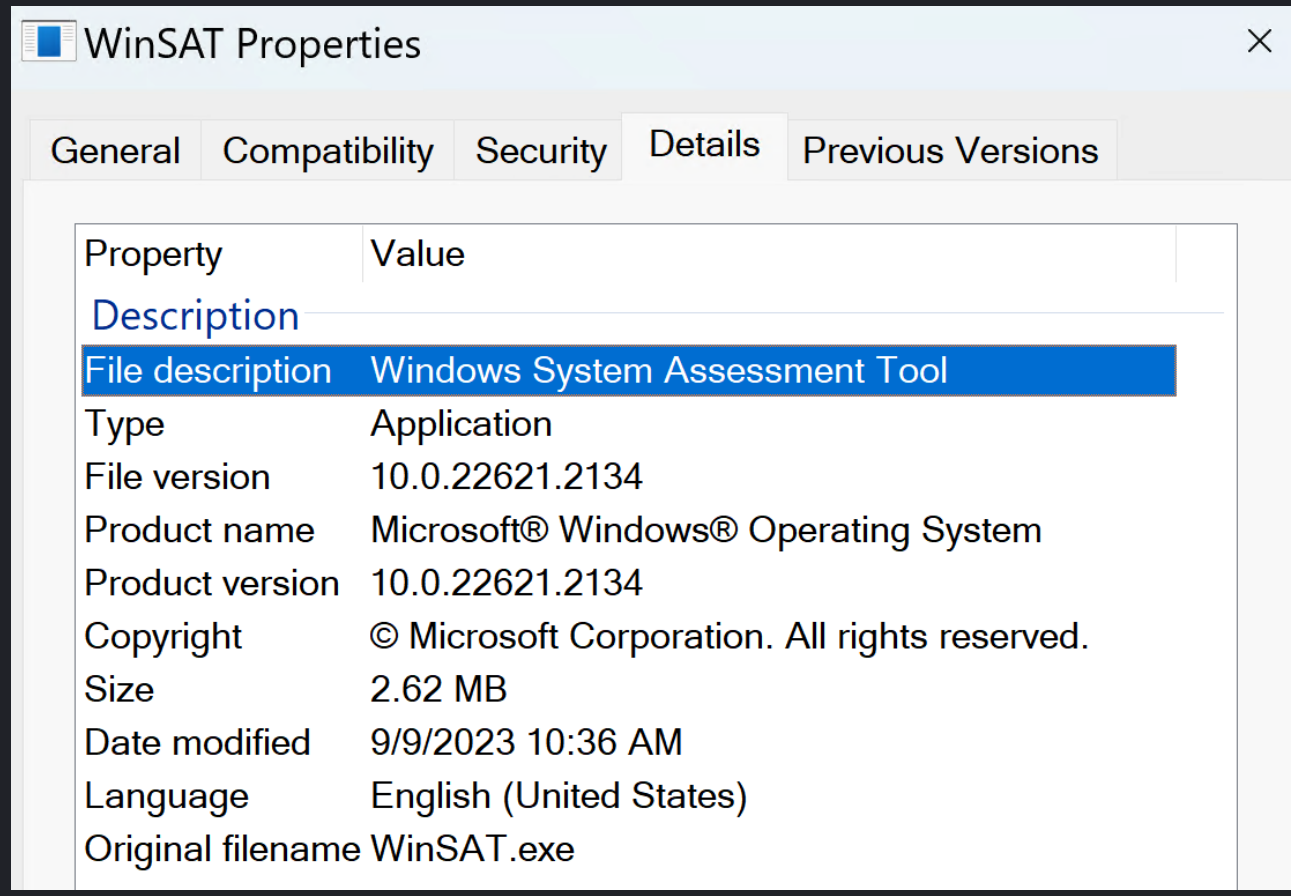
Assigning CNA: Microsoft

CVE-2023-36903

Impact: Elevation of Privilege Max Severity: Important

CVSS:3.1 7.8 / 6.8


WinSAT


WinSAT Properties
General
Compatibility
Security
Details
Previous Versions
Property
Value
Description
File description
Windows System Assessment Tool
Type
Application
File version
10.0.22621.2134
Product name
Microsoft® Windows® Operating System
Product version
10.0.22621.2134
Copyright
© Microsoft Corporation. All rights reserved.
Size
2.62 MB
Date modified
9/9/2023 10:36 AM
Language
English (United States)
Original filename
WinSAT.exe

1. Download `winsat.exe` (vulnerable and patched):

```
wget https://msdl.microsoft.com/download/symbols/WinSAT.exe/621EF9E1353000/WinSAT.exe -O winsat.exe.x64.10.0.10240.19235
wget https://msdl.microsoft.com/download/symbols/WinSAT.exe/64CABA8A354000/WinSAT.exe -O winsat.exe.x64.10.0.10240.20107
```

2. Run `ghidriff`:

```
ghidriff winsat.exe.x64.10.0.10240.19235 winsat.exe.x64.10.0.10240.20107
```

- Added
  - DeleteFileViaDisposition
  - KERNEL32.DLL::GetFileInformationByHandleEx
  - KERNEL32.DLL::SetFileInformationByHandle
  - KERNEL32.DLL::GetFinalPathNameByHandleW
- Modified
  - RemoveAllWinsatTemporaryFilesV2

RemoveAllWinsatTemporaryFilesV2 Called Diff

```diff
--- RemoveAllWinsatTemporaryFilesV2 called
+++ RemoveAllWinsatTemporaryFilesV2 called
@@ -1,2 +1 @@
-KERNEL32.DLL::DeleteFileW
-KERNEL32.DLL::GetLastError
+DeleteFileViaDisposition
```

deleted strings → added strings RENAMED

Viewed

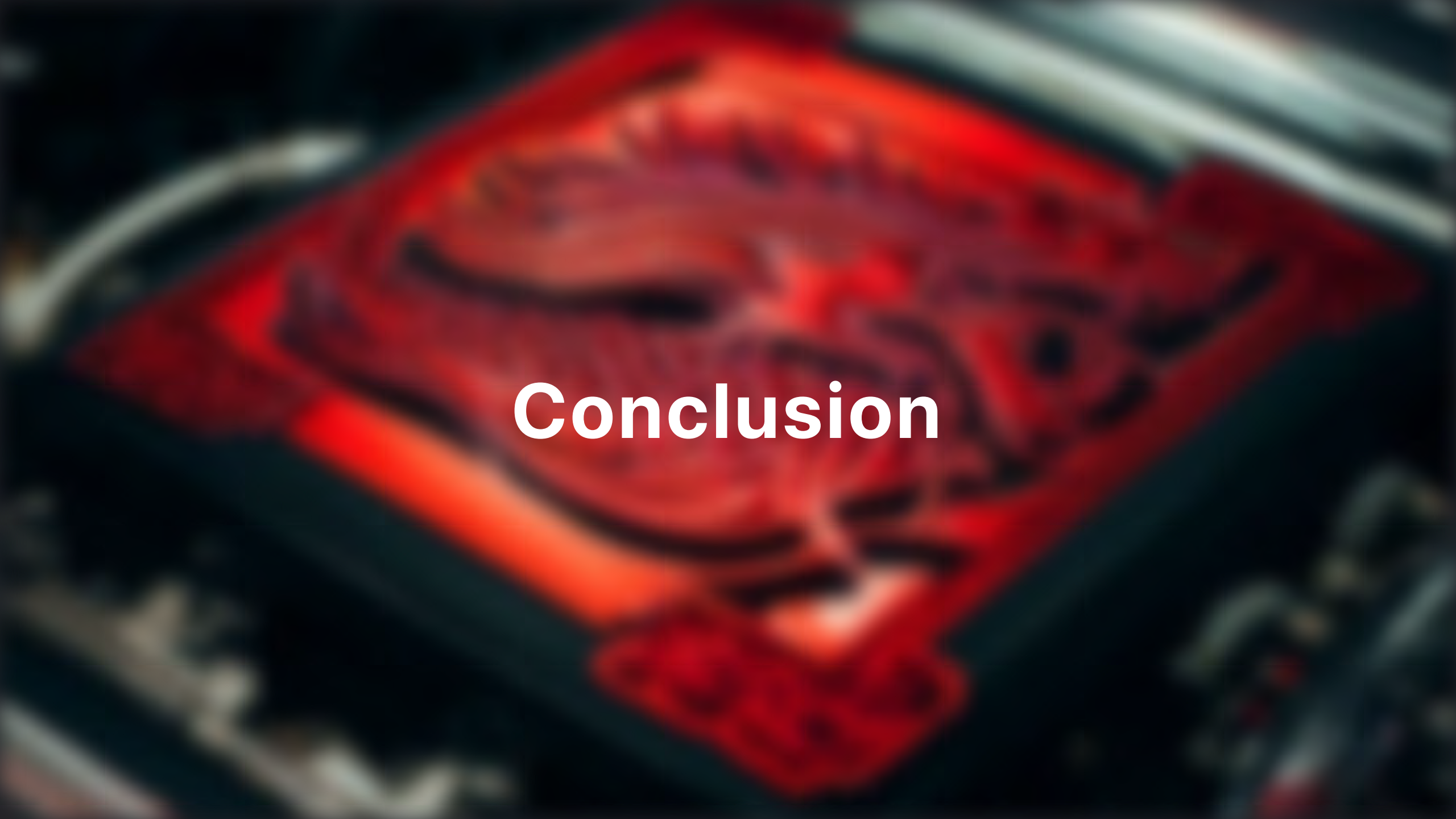
```diff
@@ -0,0 +1,2 @@
+ u_Unable_to_delete_
+ s_:_found_to_be_a_symlink
```

RemoveAllWinsatTemporaryFilesV2 Diff

```diff
--- RemoveAllWinsatTemporaryFilesV2
+++ RemoveAllWinsatTemporaryFilesV2
@@ -1,101 +1,97 @@

 /* unsigned long __cdecl RemoveAllWinsatTemporaryFilesV2(unsigned short const * __ptr64) */

 ulong __cdecl RemoveAllWinsatTemporaryFilesV2(ushort *param_1)

 {
   longlong lVar1;
   fundamental_string<ushort,class_mlib::m_traits<ushort>,class_std::allocator<ushort>_>
   *pfVar2;
   ulong uVar3;
-  BOOL BVar4;
   fundamental_string<ushort,class_mlib::m_traits<ushort>,class_std::allocator<ushort>_>
-  *pfVar5;
+  *pfVar4;
   longlong local_res10;
-  longlong local_res18;
+  longlong local_res18 [2];
```

```
(fundamental_string<ushort,class_mlib::m_traits,class_std::allocator>
                    *)(local_38._8_8_ + -8);
          }
-         BVar4 = DeleteFileW(*(LPCWSTR *)(lVar1 + 0x18));
-         if (BVar4 == 0) {
-           uVar3 = GetLastError();
-         }
+         uVar3 = DeleteFileViaDisposition(*(ushort **)(lVar1 + 0x18));
          mlib::
```

CVE-2023-36903 == Arbitrary Delete



Conclusion

`ghidriff` isn't perfect, but it is good

Known Issues

- Consistent pseudo code output
- Missing well known matching heuristics
- Needs more test automation

Filters | is:issue is:open

16 Open | 21 Closed | Author | Label

- Provide count refs for modified functions
  #45 opened 15 hours ago by clearbluejar
- Fix linting for package
  #43 opened 3 days ago by clearbluejar
- Add ability to port symbol names from one bin to another enhancement
  #42 opened on Jul 10 by clearbluejar
- Add pytest suite
  #41 opened on Jul 10 by clearbluejar 2 of 5 tasks
- Add pcode correlator
  #40 opened on Jul 10 by clearbluejar
- Add ability to create VT Session from ghidriff diff session enhancement
  #39 opened on Jul 10 by clearbluejar
- Add Version Tracking session import file support enhancement
  #31 opened on Jun 1 by clearbluejar

Unique Benefits

- Simple
- Entire stack open source
- Command line
- Social

Coming Soon

- Callgraphs
- Support custom Ghidra GDTs
- Improved documentation
- More automated testing

Patch Diffing can provide the insight you need to understand modern vulnerabilities.

`ghidriff` can help make that process a bit easier

Try It

- Find a CVE of interest
- Download the relevant binaries
- Patch diff and see what you can learn

Summary

- Binary Diffing
- Background / Motivation
- ghidriff
  - Internals
  - Features
  - CVE diffing

Questions?

github.com/clearbluejar/ghidriff