There's a lot going on here, let's look at this diagrammatically:

This function allocates and initializes a kernel

make three variable-sized kernel heap allocations:

stack buffer, and

recvmsg_x heap groom

The only hint to what's going on is that the number of loop iterations is set by a value read

userclients. The first argument is the mach port name which represents this userclient

memory; the next step in the exploit is to use the

it inherits from

External methods are numbered and can take variable sized input arguments. We'll look in

there's only one (or a small number) of

The

An IOKit driver which wishes to communicate with userspace in some way consists of two

of new code.

building memory disclosure primitives from memory corruption vulnerabilities. We'll see both

length

The

They read the

Note that the second fetch of

fetch 2:

for (i = 0; i < n_entries; i++) {

struct sub_desc* desc = &input->descs[0];

POINTER

0,

1,          // number of scalar inputs

AGXAllocationList2::initWithSharedResourceList

iPhone 9,*:

14B72 (10.1 - 24 Oct 2016)

iPhone9,4 (7 plus, D111AP)

iPhone9,3 (7, D101AP)

iPhone6,2 (5s, N53AP)

iPhone6,1 (5s, N51AP)

this group had a capability against a fully patched iPhone for at least two years.

This exploit provides evidence that these exploit chains were likely written

contemporaneously with their supported iOS versions; that is, the exploit techniques which

Exploiting CVE-2014-0556 in

What is a “good”

One Perfect Bug: Exploiting Type

One font vulnerability to rule

the life of Project Ze...

Project Zero Prize Conclusion

Exploiting .NET Managed DCOM

Over The Air - Vol. 2, Pt. 1:

Windows Exploitation Tricks:

Drawing Outside the Box:

Adventures in Video

In-the-wild iOS Exploit Chain 1

In-the-wild iOS Exploit Chain 2

Mitigations are attack surface,