CVE-2020-3845: Use-after-free in AppleSNFBUserClient

Zhuo Liang

Qihoo 360 Vulcan Team

February 24, 2020

The Safari WebContent process in macOS is capable of talking to **AppleSNFBUserClient** according to the sandbox profile. **AppleSNBFBUserClient** handle, which is available through the IOService **AppleMEClientController**, failed to handle the memory pressure issue.

Listing 1: WebProcess profile

```
(allow iokit-open
   (with report) (with telemetry)
   (iokit-registry-entry-class "AppleIntelMEUserClient")
   (iokit-registry-entry-class "AppleSNBFBUserClient"))
```

In **AppleSNBFBUserClient::start()**, the command processor **AppleMEClientController::doCmdAction()** will be called with selector 0x100. Firstly a queue will be created by **AppleMEClientController::createQueue()** in this selector. Subsequently, the queue would be appended to a linkd list attached to the IOService **AppleMEClientController** object. Then, the controller would map a segment of kernel memory with size **0x1000** into current task's map.

Unluckily, the map routine **IOMemoryDescriptor::createMappingInTask()** could fail when the userspace process is run out of memory. Once failed the queue would be destroyed but it would never be removed from the controller's linked list. It means that the kernel maintains a linked list in which an object has already been freed.