IOActive Security Advisory

Title	Steam Client creates world-writable shell script
Severity	High
Discovered by	Ilja van Sprundel

Affected Products

Steam client for Mac OS X prior to May 21st update

Impact

While performing a routine world-writable file scan, one of IOActive's consultants discovered that the Steam Client for Mac OS X creates world-writable shell scripts when installing games:

```
iljas-MacBook-Pro:~ ilja$ sudo find / -perm -0666 -type f
find: /dev/fd/3: Not a directory
find: /dev/fd/4: Not a directory
/Library/Application Support/GarageBand/Package Registry.plist
/Library/Application Support/Microsoft/Communicator/Communicator.plist
/Library/Application Support/Microsoft/PlayReady/.Cache/indiv01.bla
/Library/Application Support/Microsoft/PlayReady/.Cache/indiv01.cat
/Library/Application Support/Microsoft/PlayReady/.Cache/indiv01.key
/Library/Application Support/Microsoft/PlayReady/.Cache/indiv01.tmp
/Library/Application Support/Microsoft/PlayReady/mspr.hds
/Library/Application Support/VMware/VMware Fusion/Shared/vmInventory
/Library/Audio/Apple Loops Index/Search Index 4B8A1BE5-1C44-4D75-BBD9-834AE2E80669.txt
/Library/Audio/Apple Loops Index/Search Index 9BB4C57A-842E-4F96-BC44-29CEC3D7F725.txt
/Library/Caches/com.apple.DiagnosticReporting.Networks.plist
/Users/ilja/Applications/Sid Meier's Civilization V.app/Contents/MacOS/run.sh
/Users/ilja/Desktop/test.c
/Users/ilja/Library/Logs/FlashPlayerInstallManager.log

iljas-MacBook-Pro:~ ilja$ ls -alhp "/Users/ilja/Applications/Sid Meier's Civilization
V.app/Contents/MacOS/run.sh"
-rwxrwxrwx  1 ilja  staff    71B Dec 15 03:55 /Users/ilja/Applications/Sid Meier's Civilization
V.app/Contents/MacOS/run.sh
iljas-MacBook-Pro:~ ilja$ cat "/Users/ilja/Applications/Sid Meier's Civilization V.app/Contents/MacOS/run.sh"
```

```
#!/bin/bash
# autogenerated file - do not edit

open steam://run/8930

iljas-MacBook-Pro:~ ilja$
```

On a multi-user system, a user could escalate his privileges to that of any user playing a game installed by the Steam Client.

Solution

This issue was fixed with the May 21st update of the Steam Client. See the following Steam webpage: http://store.steampowered.com/news/13399/