Bug Reports J. Gallagher

Bug Location: Megavideo Internet Television
Date Filed: Sunday April 5, 2011
Type of Bug: Website: Megavideo.com
Reproducible: Yes, but with some variations.
Description:

Megavideo is an online video filesharing system. People can upload videos and others can watch them. It is similar to youtube.com, but does not place as many restrictions on the nature, contents, or length of the material posted.

Megavideo does place a limit on the length of time one IP address can access the videos on their site. The time limit is 72 minutes. Megavideo has had a history of people finding ways to get around their 72 minute time limit, but all of the commonly listed mechanisms are now obsolete. The most famous of the obsolete techniques is to download the video and then watch it in offline mode. However, we have found two expressions of what appears to be a common bug that allows one to bypass the 72 minute time limit.

To Reproduce the bugs:

1. The first bug is a removal of the 72 minute time limit or a piece of it. Watch 72 minutes of Megavideo. As soon as the “You have watched 72 minutes of Megavideo today, please wait 30 minutes to continue” warning pops up, hit refresh, hit the red play button, then the green play button. Once in a while, there is no waiting at all; there is usually some removal of the wait time.
2. The second bug allows a wait time of around 5 minutes versus 30 minutes. Watch 72 minutes of Megavideo. When the “You have watched ...” warning pops up, hit refresh, and then the red button, but don't hit the green button. Wait five minutes. Hit the green button. The video plays nearly 100% of the time.

Shortcomings:

We could not get a better model of the bug from our end. All we know is that the servers are not tracking something correctly. The states, such as timestamps must be stored and computed on the server. We used several tools to monitor http messages and flash content, but no state about time was agreed on. Thus we could only alert Megavideo that their site has some flaws, but could make no recommendations as to courses of action.

Resolution:

Megavideo has been sent an email containing steps to reproduce the bug, and various expressions of the bug. We have also sent screen casts showing the bug being produced. I have yet to hear back from Megavideo.

I have many documented videos (screencasts) of the exploit, but I have omitted them here for copyright reasons. I am happy to email them though.