By Dan Goodin, TheRegister.co.uk
Twitter is sitting on an amateur configuration blunder that makes it trivial for attackers to take control of user accounts, a researcher said Friday.
The error resides in an Adobe Flash object hosted on the microblogging site, said Mike Bailey, a senior security analyst with penetration testing firm Foreground Security. Contrary to Adobe recommendations, the object is free to load files hosted virtually anywhere on the net, including those containing booby-trapped javascript and action script.

″This is not Adobe`s fault,″ Bailey told El Reg. ″This is due to the fact that a lot of really bad programmers are coding Flash objects. I`ve seen literally hundreds of these things across the web.″

The list of other offenders making the same goof reads like a who`s who of search engines, software companies and news sites. Bailey shared the names with The Register on the condition they not be published. He plans to out many of the sites during a talk scheduled for next month at the Black Hat security conference in Washington DC.

Using an XML file hosted on one of his servers, Bailey was able to exploit the weakness to cause a dummy account to tweet: ″@mckt_ just pwned my Twitter account. Neat.″ All that was required was that a link on Bailey`s server be clicked while logged in to Twitter. (As usual, the NoScript addon for Firefox blocked the exploit.)

But the consequences could have been more malicious.

″In reality, I have full access to everything your Twitter account has on the web,″ Bailey said. ″I can think of a million ways to use this as an attacker.″

Actions include adding or removing account followers and reading direct messages presumed private.

Reconfiguring an object not to talk to strange files generally takes a matter of minutes, maybe an hour or two at most. And yet, at time of writing, the flaw was still active more than 24 hours after Bailey reported it. That doesn`t give us a warm and fuzzy feeling about the site`s security.
® Update

Around the same time this article was published, Twitter said it had disabled the misconfigured Flash object ″out of an abundance of caution″ while the situation is assessed.