

Advisory : Severe Phishing And Redirection Attacks In AOL ScreenName Website

Dated : 23 November 2006

Severity : Critical

By: Aditya K Sood [www.secniche.org]

Explanation :

The screensaver AOL website is subjected to phishing attacks as the redirection is possible with manipulation in URL.



This flaw occur in the way when ever user registered to the screensaver website with login page specified as:

URL : my.screenname.aol.com/_cqr/login/aimPrelogin.psp?

The attacker exploit the URL parameters by specifying the desired website he wants to redirect as :

my.screenname.aol.com/_cqr/login/aimPrelogin.psp?siteId=HPPPProdParentAlt&siteState=redirect@<Website Name>

Example:

my.screenname.aol.com/_cqr/login/aimPrelogin.psp?siteState=redirect@http://www.slashdot.org

After the successful login the page is redirected to attackers destination. The whole site with this URL paradigm is vulnerable to these attacks.

Vendor Status :

Reported And Patched. The System after login has been subjected to more security.