



**Advisory** : Yahoo Network prone to redirection and phishing attacks.

**Dated** : 19 June 2007

**Severity** : Critical

By: Aditya K Sood [ [www.secniche.org](http://www.secniche.org) ]

**Explanation: [Yahoo Network]**

A severe redirection and phishing vulnerability have been found in Yahoo Network. The specific URL linked to any further yahoo website can be manipulated by the attacker to redirect the traffic and used for phishing. The critical point is the URL can be called by third party for phishing.

**Example :**

[Persisting Link]

[https://us.ard.yahoo.com/SIG=12gb00bbf/M=341232.9804850.11489914.6055752/D=regst/S=150001465:R2/Y=YAHOO/EXP=1182284104/A=4651436/R=0/SIG=1255of0p5/\\*http://help.yahoo.com/l/us/yahoo/mail/yahoomail/tools/tools-08.html](https://us.ard.yahoo.com/SIG=12gb00bbf/M=341232.9804850.11489914.6055752/D=regst/S=150001465:R2/Y=YAHOO/EXP=1182284104/A=4651436/R=0/SIG=1255of0p5/*http://help.yahoo.com/l/us/yahoo/mail/yahoomail/tools/tools-08.html)  
[http://us.ard.yahoo.com/SIG=12l25b5lf/M=289534.9533254.10260072.9228191/D=sec\\_cntr/S=565000002:FOOT/Y=YAHOO/EXP=1182284340/A=4080514/R=0/SIG=11lp7krcc/\\*http://docs.yahoo.com/info/copyright/copyright.html](http://us.ard.yahoo.com/SIG=12l25b5lf/M=289534.9533254.10260072.9228191/D=sec_cntr/S=565000002:FOOT/Y=YAHOO/EXP=1182284340/A=4080514/R=0/SIG=11lp7krcc/*http://docs.yahoo.com/info/copyright/copyright.html)

The network is us.ard.yahoo.com. The vulnerability persist in the internal redirection directly from website or from third party. the attacker manipulates it as :

[Linking URL]

<https://us.ard.yahoo.com/SIG=12gb00bbf/M=341232.9804850.11489914.6055752/D=regst/S=150001465:R2/Y=YAHOO/EXP=1182284104/A=4651436/R=0/SIG=1255of0p5/>< Rogue WebsiteName>

[Manipulated URL]

[https://us.ard.yahoo.com/SIG=12gb00bbf/M=341232.9804850.11489914.6055752/D=regst/S=150001465:R2/Y=YAHOO/EXP=1182284104/A=4651436/R=0/SIG=1255of0p5/\\*http://www.google.com](https://us.ard.yahoo.com/SIG=12gb00bbf/M=341232.9804850.11489914.6055752/D=regst/S=150001465:R2/Y=YAHOO/EXP=1182284104/A=4651436/R=0/SIG=1255of0p5/*http://www.google.com)

[https://us.ard.yahoo.com/SIG=12gb00bbf/M=341232.9804850.11489914.6055752/D=regst/S=150001465:R2/Y=YAHOO/EXP=1182284104/A=4651436/R=0/SIG=1255of0p5/\\*http://www.hushmail.com](https://us.ard.yahoo.com/SIG=12gb00bbf/M=341232.9804850.11489914.6055752/D=regst/S=150001465:R2/Y=YAHOO/EXP=1182284104/A=4651436/R=0/SIG=1255of0p5/*http://www.hushmail.com)

The whole network is vulnerable to this. It is a virtually manipulated.

**Status** : Patched Within 24 hours.