

Advisory : Phishing Vulnerability in Yahoo Search Engine.

Dated : 19 June 2007

Severity : Critical

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

Explanation: [Yahoo Search]

A severe redirection and phishing vulnerability have been found in Yahoo Search Network. The links provide for the search to next page can be manipulated by the phishers to redirect traffic and used yahoo search engine for phishing. The vulnerability affects the yahoo search engine at full.

[Persistent Link] : The category of links that are affected.

Example:

http://rds.yahoo.com/_ylt=A0geu4qjI3hGYOEAIjJXNyoA/SIG=14oi6m38j/EXP=1182364963/**http%3a//search.yahoo.com/search%3fp=Hacking%26y=Search%26rd=r1%26meta=vc%253Din%26fr=yfp-t-501%26fp_ip=IN%26xargs=0%26pstart=1%26b=11

http://rds.yahoo.com/_ylt=A0geu4qjI3hGYOEAIzJXNyoA/SIG=14o91b3v5/EXP=1182364963/**http%3a//search.yahoo.com/search%3fp=Hacking%26y=Search%26rd=r1%26meta=vc%253Din%26fr=yfp-t-501%26fp_ip=IN%26xargs=0%26pstart=1%26b=21

YAHOO! SEARCH 1 2 3 4 5 6 7 8 9 10 ▶ **Next**

zeroknock

Search

The above stated URL's are taken from the next page of query set as "zeroknock". The network used is rds.yahoo.com. The phisher exploits it by stripping off full yahoo search and appending the rogue website.

[Original URL]

http://rds.yahoo.com/_ylt=A0geu4qjI3hGYOEAIjJXNyoA/SIG=14oi6m38j/EXP=1182364963/**http%3a//search.yahoo.com/search%3fp=Hacking%26y=Search%26rd=r1%26meta=vc%253Din%26fr=yfp-t-501%26fp_ip=IN%26xargs=0%26pstart=1%26b=11

[Phishing URL]

[http://rds.yahoo.com/_ylt=A0geu4qjI3hGYOEAIjJXNyoA/SIG=14oi6m38j/EXP=1182364963/**http%3a//\[Phishing Website\]](http://rds.yahoo.com/_ylt=A0geu4qjI3hGYOEAIjJXNyoA/SIG=14oi6m38j/EXP=1182364963/**http%3a//[Phishing Website])
http://rds.yahoo.com/_ylt=A0geu4qjI3hGYOEAIjJXNyoA/SIG=14oi6m38j/EXP=1182364963/**http%3a//www.metasploit.com

The whole yahoo search engine is vulnerable to this. The problem persist in the internal linking.

Vendor Status: Reported. Accepted. Patch is in progress as explained by yahoo security.