



Advisory : Phishing Vulnerability in Google News Network.

Dated : 15 October 2007

Severity : Critical

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

Explanation: [Google News]

A severe redirection and phishing vulnerability have been found in Google News Network. The URL can be used to launch third party attacks. An attacker can exploit it for malicious purposes. This type of exploitation parameter enables phishers to redirect traffic.

Example :

[Persisting Link]

http://news.google.com/news/url?sa=t&ct=us/8-2-3&fp=4711b21fd5c60842&ei=ryIRR-yWJozQqgOR6_HeDQ&url=http%3A//ap.google.com/article/ALeqM5hQJTz5etV1jS5HS2aFExRoauSbWQD8S82GFO1&cid=1122015172

The vulnerability persist in the internal redirection directly from website or from third party. the attacker manipulates it as :

[Linking URL]

http://news.google.com/news/url?sa=t&ct=us/8-2-3&fp=4711b21fd5c60842&ei=ryIRR-yWJozQqgOR6_HeDQ&url=[Rogue URL]

[Manipulated URL]

http://news.google.com/news/url?sa=t&ct=us/8-2-3&fp=4711b21fd5c60842&ei=ryIRR-yWJozQqgOR6_HeDQ&url=http://www.msn.com

http://news.google.com/news/url?sa=t&ct=us/8-2-3&fp=4711b21fd5c60842&ei=ryIRR-yWJozQqgOR6_HeDQ&url=http://www.packetstormsecurity.org

The whole network is vulnerable to this.

Vendor Status : Notified to Google. Acknowledged.