

Advisory : Phishing and Redirection Issue in Google Translation

Dated : 5 January 2007

Severity : Intermediate

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

Explanation: [Google]

The translate Google is a service that is provided by Google to translate web pages to the desired language. The prime functioning depends on the factor that a web page of different language is selected and translate in to user specific choice. The definitive URL as mentioned:

<http://translate.google.com/translate?hl=en&sl=ja&u=>

If we strip the parameter arguments it will be undertaken as:

hl=> The language in which translation to be done

sl=> The Source language

u=> The URL to be translated

Since the redirection vulnerability persist in the layout as if we strip off the parameters of [hl]& [sl] and provide direct URL to the parameter [u] it redirects the traffic in the domain context.

The default parameter URL:

<http://translate.google.com/translate?hl=en&sl=ja&u=>

The stripped Off parameter URL:

<http://translate.google.com/translate?u=>

Example:

<http://translate.google.com/translate?u=http://www.packetstormsecurity.org>

Vendor Status:

It has been reported to Google. Acknowledged fully. Patched after 6-8 months.