

Advisory :

Skype IM Client Password Disclosure Vulnerability.

Version Affected:

Skype 3.8 / Previous version can be affected.

Release Date:

11 September 2008

Description:

The skype client inherits client side password disclosure vulnerability. The credentials used to connect to the required service i.e. username and password is not encrypted properly. The credentials can be extracted in clear text by dumping process memory of the live skype process when a connection is set. The vulnerability allows anyone with access to the client system to obtain the username and password. Additionally, this vulnerability could also be exploited by fooling the user to execute malicious code which would dump the memory of the process "skype.exe". The skype uses skype.exe and skypepm.exe processes while communicating. The skype.exe dumps password in clear text.

Proof of Concept:

Download: http://www.evilmfingers.com/advisory/skype_pass_dis_vul.pdf

Credit:

Aditya K Sood

Team Lead, www.EvilFingers.com

<http://www.secniche.org>

Disclaimer

The information in the advisory is believed to be accurate at the time of publishing based on currently available information. Use of the information constitutes acceptance for use in an AS IS condition. There is no representation or warranties, either express or implied by or with respect to anything in this document, and shall not be liable for any implied warranties of merchantability or fitness for a particular purpose or for any indirect special or consequential damages.