

Advisory:

Miranda IM Client Password Disclosure Vulnerability.

Version Affected:

Miranda 0.7.10 Unicode - Miranda IM is a multi-protocol instant messaging client for Windows. Very light on system resources and extremely fast, Miranda IM require no installation and can be made to fit on a single floppy disk or USB drive. Featuring a powerful plugin-based framework and boasting over 350 plugins, Miranda IM is one of the most flexible and customizable messaging clients on the planet.

Release Date:

11 September 2008

Description:

The Miranda 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 miranda 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 "miranda32.exe".

Proof of Concept:

Download: http://www.evilfingers.com/advisory/miranda_im_mem_pass_disc.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.