Hamachi VPN Client 1.0.2.5 Password Disclosure Vulnerability

Discovered by: Giuseppe Bonfa' alias Evilcry

E-Mail: evilcry@gmail.com

WebSite: http://evilcry.altervista.org

Risk: Not Critical

Impact: Exposure of sensitive informations

Where: From local network

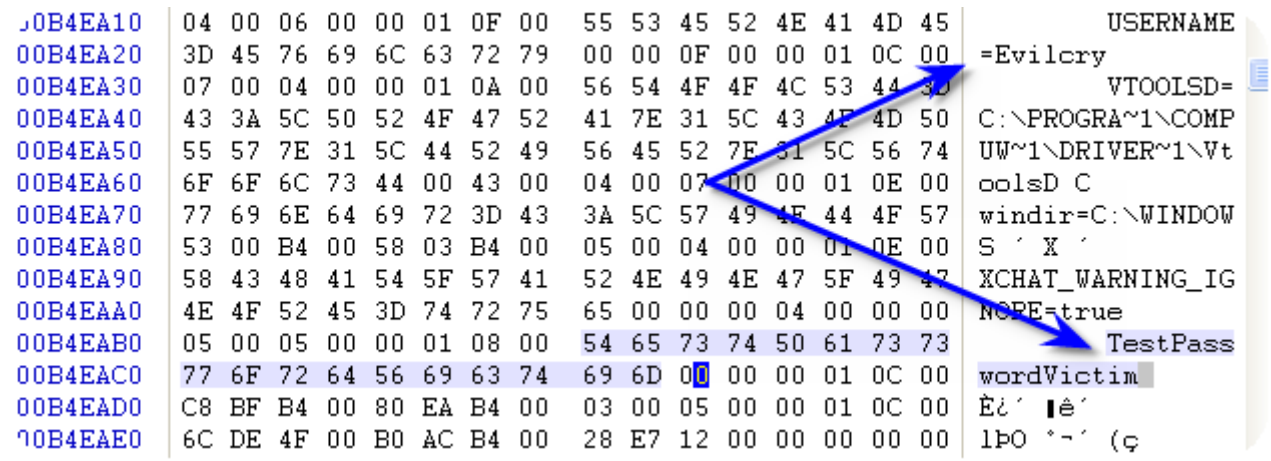
Solution Status: Not Fixed

Date: 24-03-2008

Description

Hamachi is a Client for Trusted VPN Tunneling.
It presents a Password Disclosure Vulnerability, because User and Passwords are not correctly protected for Memory Sniffing Attacks, so a local attacker, with a basilae Process Memory Dumper, could obtain the Connection Password.

Here a little demonstration of the vulnerability:



It's easy to locate password, hamatchi presents some costant strings, such as 'USERNAME' and 'XCHAT_WARNING_IGNORE='.