

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:

00B4EA10	04 00 06 00 00 01 0F 00	55 53 45 52 4E 41 4D 45	USERNAME
00B4EA20	3D 45 76 69 6C 63 72 79	00 00 0F 00 00 01 0C 00	=Evilcry
00B4EA30	07 00 04 00 00 01 0A 00	56 54 4F 4F 4C 53 44 40	VTOLSD=
00B4EA40	43 3A 5C 50 52 4F 47 52	41 7E 31 5C 43 4F 4D 50	C:\PROGRA~1\COMP
00B4EA50	55 57 7E 31 5C 44 52 49	56 45 52 7E 31 5C 56 74	UW~1\DRIVER~1\Vt
00B4EA60	6F 6F 6C 73 44 00 43 00	04 00 07 00 00 01 0E 00	oolsD C
00B4EA70	77 69 6E 64 69 72 3D 43	3A 5C 57 49 4F 44 4F 57	windir=C:\WINDOW
00B4EA80	53 00 B4 00 58 03 B4 00	05 00 04 00 00 01 0E 00	S ' X '
00B4EA90	58 43 48 41 54 5F 57 41	52 4E 49 4E 47 5F 49 47	XCHAT_WARNING_IG
00B4EAA0	4E 4F 52 45 3D 74 72 75	65 00 00 00 04 00 00 00	NOPE=true
00B4EAB0	05 00 05 00 00 01 08 00	54 65 73 74 50 61 73 73	TestPass
00B4EAC0	77 6F 72 64 56 69 63 74	69 6D 00 00 00 01 0C 00	wordVictim
00B4EAD0	C8 BF B4 00 80 EA B4 00	03 00 05 00 00 01 0C 00	È' 'è'
00B4EAE0	6C DE 4F 00 B0 AC B4 00	28 E7 12 00 00 00 00 00	lBO '-' (q

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