

[Full-Disclosure] Prrivacy Vunerability Ifriends IFCAM96D

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-03/0208.html>

From: Hotmail (se_cur_itv@hotmail.com)

Date: 03/23/03

From: "Hotmail" <se_cur_itv@hotmail.com>

To: <Full-Disclosure@lists.netsys.com>

Date: Sun, 23 Mar 2003 01:11:42 -0800

For the past year Ifriends.com (WP Associates) has known about a security compromise in its chathost software ifcam96d. The program is coded in such a way, and the structure of Ifriends.com Java/Browser based traction scheme that makes it possible to bypass all security measures and payment, allowing compromised viewing of private chathost sessions. I will briefly detail the problem, the compromise, and the resolve taken as of this posting. Ifcam96d is a software platform for dellivering private, live, pay per view adult content. Examining the ifcam.exe binary in Bintext or similar, reveals that the program is comprised of a combination of VB, Java and HTML code. Simply by examining this, making a text copy of the binary and subsituting a file name present in a java class for a parameter in the applet tags, presents you with a crude but effective viewer for these "private shows". With only the information for ip address and port of any operating ifcam setup, this allows you total view of the chathosts webcam video. This is a serious Privacy Violation in direct contrast to WP/Ifriends own statements at <http://www.ifriends.net/experts/toursexcursions.htm> and I quote ". It's called a "one-to-one" connection. And it guarantees privacy for both you and the customer. Nobody can snoop and watch for free." . Indeed it is a "one-to-one" connection and viewing is possible without the parent company aware that this is taking place. In Jan 2002 I personally retained a lawyer to contact WP associates regarding a chathost(me), that had noticed people were viewing thier cam although I was not logged into thier service, meerly having the software running. Thier reply at that date was "we are aware of the problem and there really nothing we can do for you, sorry" Further examination reveals embedded ip addresses that informs ifriends that the software is running even if not logged in, full unrestricted access to you video at any time, and the ability to send a "please return to your cam" announce ability. Finaly there is an undocumented access port 7903. Webpower Inc has been informed of a development of a proof of concept program, CamScam screenshot to fully exploit these flaws and to show the lack of privacy commitment of a very large internet company. They were offered the oportunity to have us develop this into an integrated part of their operation as it can be modified very easily to thier specifications and completly would remove the vulnerability that exists. As of March 14 4:25 pm Ifriends has released a new version of thier chathost software, addressing some of these issues while not completly curing the problem. As well.. Upon review of thier public and chathost forums, I see they have not taken the steps to inform thier members/hosts of the privacy issues discussed here. Full exploit info and discussion available, contact: morningwood@thepub.co.za Pro Active Security <http://take.candyfrom.us> <http://mywood.kicks-ass.org/thcore/>

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>