The Win32 Hotline Server, produced by Hotline Communications, Ltd. and hxd have a security hole which allows anyone with access to hx or MacsBug to gain entry to the entire server hard drive. The glitch is merely a matter of taking advantage of the file systems directory structure, and accessing "/..", which leads to a higher directory. THC was able to gain access to several servers, and on those which had download privileges enabled for guests we were able to download user data files, Hotline bookmarks and various other files which some would consider to contain sensitive information. If you feel your server is at risk with this security hole we recommend you move your server to a MacOS alternative immediately.

hx

With hx, the intruder need only to change the directory character to something besides "/". The command to change it to ":" is:

```
/dirchar :
```

After that, simply changeing directories to "/.." over and over will let them reach higher levels of the directory tree. ie -

```
/cd "/.."
```

Note: THC was only able to complete the hack with hx 0.7.9. The only other version which we have access to (0.5.28) does not have the dirchar command.

MacsBug

With MacsBug, the intruder will have to open a folder, then search for that name in memory, then modify it.

The search command is:

```
f address numberOfBytes 'text'
```

Where "address" is the address displayed by the "hz" command, and "numberOfBytes" is just a large number (like a couple of megabytes).

When it finds it, it displays what it found and the address. The intruder can then change it using "sb".

Obviously the intruder will need to change the name to "/..", but they also need to set the byte immediately preceding to 3.