NUL CHARACTER CERTIFICATE ATTACK 090731

An attack has been developed against many implementations of SSL used in browsers (see `www.wired.com/threatlevel/2009/07/kaminsky/`). The attack is against the *implementation*, not the protocol; in particular, the attack is against certain implementations of the code that performs certificate checking. The same attack can reasonably assumed to work against other implementations of the same function in protocols other than SSL. PacketCable-based security systems perform this function as part of the initial authentication exchange.

The attack works because (apparently) some certificate-checking software in widespread use has been written by developers who are unaware how to correctly handle strings that contain an embedded ASCII NUL character (*i.e.*, eight bits with the value zero).

We wish to assure our customers that the IPfonix Inc., KDC software is immune to this attack, just as it is immune to the issues in the pointer-related security bulletins that have affected other implementations of Kerberos in the past.

The author of our software, in addition to serving on security focus teams for the cable environment, was also a member of the C++ standardization committee., and consequently has considerable expertise in understanding and proactively preventing possible programming errors of the type revealed by this attack. This type of attack is just one of many against which the IPfonix KDC has been designed since the very beginning.

Since our first deployment in the early 2000s, we are unaware of any successful attack against our code. We would like to take this opportunity to thank our customers for putting their trust in us, and assure them that we take that trust very seriously indeed.