Suresec security advisory 6
5th September 2005
CVE IDs: CAN-2005-2494

Insecure file operation in kcheckpass

Vulnerability summary:
kcheckpass is a utility used to authenticate users. It's used by tools such as kscreensaver. The code that's used to create a lockfile doesn't check for or sets the umask. Besides the umask problem it will also happily follow symlinks, as shown by the following code snippet:

```
...
sprintf(fname, "/var/lock/kcheckpass.%d", uid);
if ((lfd = open(fname, O_RDWR | O_CREAT)) >= 0) {
     ...
}
...
```

In order for an attacker to be able to exploit this /var/lock would have to be world writable and kcheckpass would have to be suid. When these conditions are met an attacker can create a world writable file anywhere.

Impact:
When properly exploited users can gain root privileges (given that the previously mentioned conditions are met).

Affected versions:
kdebase 3.2.0 till 3.4.2 are affected by this vulnerability.

Suggested Recommendations:
apply the kde security update for kdebase (post-3.4.2-kdebase-kcheckpass.diff).

Credits:
Ilja van Sprundel found this vulnerability.

About us:
Suresec Ltd is a global service provider of Internet security solutions and consultancy with unmatched quality from our world class consultancy practice.

Our consultants have pioneered in the field of security research and have closely worked with leading software companies and service providers to mitigate risks and fix a number of critical vulnerabilities, Suresec also works closely with a number of open source companies
to provide them with a source code auditing and technical consultancy. We have a strong team consultants spread across Europe, the United States of America And Australia specializing in security consulting.