

[UNIX] kcheckpass Insecure File Operation

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-09/0090.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/26/05

To: list@securiteam.com

Date: 26 Sep 2005 11:06:32 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

kcheckpass Insecure File Operation

SUMMARY

<<http://kde.org>> kcheckpass – KDE pam client that allows you to auth as a specified user without actually doing anything as that user.

kcheckpass creates lockfile in an insecure way, exploiting this vulnerability allows malicious attacker to create a world writable file anywhere.

DETAILS

Vulnerable Systems:

* kdebase versions 3.2.0 to 3.4.2

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) {
}
..
```

Securiteam: [UNIX] kcheckpass Insecure File Operation

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.

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

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2494>>
CAN-2005-2494

ADDITIONAL INFORMATION

The information has been provided by <<mailto:advisories@suresec.org>> Ilja van Sprundel.

The original article can be found at:

<<http://www.suresec.org/advisories/adv6.pdf>>
<http://www.suresec.org/advisories/adv6.pdf>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.