

[UNIX] KDM Vulnerabilities (pam_setcred, session cookie)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-09/0058.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/17/03

To: list@securiteam.com

Date: 17 Sep 2003 13:58:34 +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>

KDM Vulnerabilities (pam_setcred, session cookie)

SUMMARY

Two issues have been discovered in KDM:

- a) Privilege escalation with specific PAM modules
- b) Session cookies generated by KDM are potentially insecure

KDM does not check for successful completion of the `pam_setcred()` call. In case of error conditions in the installed PAM modules, KDM might grant local root access to any user with valid login credentials.

It has been reported that a certain configuration of the MIT `pam_krb5` module can result in a failing `pam_setcred()` call leaving the session alive and providing root access to a regular user.

Additionally the session cookie generation algorithm used by KDM was considered too weak to supply full 128 bits of entropy. This enables non-authorized users to brute-force the session cookie.

DETAILS

Vulnerable systems:

Securiteam: [UNIX] KDM Vulnerabilities (pam_setcred, session cookie)

All versions of KDM as distributed with KDE up to and including KDE 3.1.3.

Impact:

If KDM is used in combination with the MIT pam_krb5 module and given a valid username and password of an existing user, the login attempt succeeds and establishes a session with excessive privileges. This may enable a local root compromise of the system.

It is possible that the same vulnerability exists if KDM is used with other PAM modules. At the date of this advisory we are however not aware of any other PAM module being affected by this vulnerability.

The weak cookie generation may allow non-authorized users to guess the session cookie by a brute force attack, which allows, assuming hostname / IP restrictions can be bypassed, to authorize to the running session and gain full access to it.

Solution:

a) Privilege escalation with specific PAM modules:

The patch listed in section 5 adds error checking to KDM and aborts the login attempt if an error occurs during the pam_setcred() call.

There is no intermediate workaround known. Users who do not use PAM with KDM and users who use PAM with regular UNIX crypt/MD5 based authentication are not affected.

b) Weak cookie generation:

The patch listed in section 5 adds a new cookie generation algorithm, which uses /dev/urandom as non-predictable source of entropy.

Users of KDE 2.2.2 are advised to upgrade to KDE 3.1.4. A patch for KDE 2.2.2 is available for users who are unable to upgrade to KDE 3.1.

Users of KDE 3.0.x are advised to upgrade to KDE 3.1.4. A patch for KDE 3.0.5b is available for users who are unable to upgrade to KDE 3.1.

Users of KDE 3.1.x are advised to upgrade to KDE 3.1.4.

Patch:

A patch for KDE 2.2.2 is available from
<ftp://ftp.kde.org/pub/kde/security_patches>
ftp://ftp.kde.org/pub/kde/security_patches:

4672868343b26e0c0eae91ffeff1f7e post-2.2.2-kdebase-kdm.patch

A patch for KDE 3.0.5b is available from
<ftp://ftp.kde.org/pub/kde/security_patches>
ftp://ftp.kde.org/pub/kde/security_patches:

fde237203fc7b325c34d2f90a463db3f post-3.0.5-kdebase-kdm.patch

Securiteam: [UNIX] KDM Vulnerabilities (pam_setcred, session cookie)

A patch for KDE 3.1.3 is available from
<ftp://ftp.kde.org/pub/kde/security_patches>
ftp://ftp.kde.org/pub/kde/security_patches:

8553c20798b321e333d8c516636f2297 post-3.1.3-kdebase-kdm.patch

Time line and credits:

- 12/06/2002 Posting on suse-security mailing list describing the PAM vulnerability.
- 08/06/2003 Notification of KDE Security and the KDM maintainer about the PAM vulnerability by Stephan Kulow.
- 08/09/2003 Patches for the PAM vulnerability applied to KDE CVS.
- 08/20/2003 George Lebl notifies Oswald Buddenhagen about weak session cookie generation in KDM.
- 08/26/2003 Impact analysis and advisory finished.
- 09/04/2003 Patches for the weak cookie vulnerability applied to CVS.
- 09/16/2003 Public advisory.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:mueller@kde.org>> Dirk Mueller.

=====

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.