

[UNIX] Cleartext SMB Passwords in Novell Desktop Linux using KDE

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-12/0083.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/22/04

To: list@securiteam.com

Date: 22 Dec 2004 15:09:49 +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>

Cleartext SMB Passwords in Novell Desktop Linux using KDE

SUMMARY

Novell Desktop Linux has been found to contain a vulnerability that causes it to store the SMB username and password in clear text, this would allow a local attacker to easily recover the password used for SMB logon.

DETAILS

Systems affected:

Novell Desktop Linux 9 when using KDE (release 3.2.1). Other distributions with KDE may be affected as well. Mike couldn't reproduce this on Fedora Core 3. Mike tried performing the same action on Novell Desktop Linux 9 with Gnome, but the GUI wouldn't let me create a symbolic link to a shared file/folder. Mike is not sure if other distributions are affected.

Temporary workaround:

Don't create symbolic links to networked files and folders if using KDE. The correct thing for the system to do is not put the username and password information in the filename, meta data or URL field. These should either be stored in an encrypted key repository (like Apple's

Securiteam: [UNIX] Cleartext SMB Passwords in Novell Desktop Linux using KDE

Keychain) or requested every time the user accesses the network share.

Vendor status:

Contact with Novell occurred on November 16, 2004. Vendor claims a fix should be out soon.

Exploit:

When creating a symbolic link to a file or folder located on a SMB network share using KDE, the user's name and password are displayed in clear text on the desktop. The login name and password are also in the link file's meta data in addition to the actual filename itself.

Steps to perform the exploit:

- * Install NLD with KDE (either default to KDE or choose to install both KDE and Gnome)
- * Log in via KDE
- * Open Network Browser
- * Open Windows Network
- * Find an SMB Windows share
- * Authenticate to the share
- * Left click on a file or folder, drag it to the desktop, select "Link Here"
- * A file will be created on the desktop

File name is:

smb://username:password@server/path/to/file

It puts the username and password both in clear text on the desktop, in plain site of everyone. These also appear in the URL and Meta Info property location. When Mike tried doing that in Gnome, Mike got a message "Error 'Unsupported operation' while creating a link to smb://server/path/to/file" and it doesn't create the link.

ADDITIONAL INFORMATION

The information has been provided by <mailto:mdemaria@nwc.com> Mike DeMaria.

=====

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,

Securiteam: [UNIX] Cleartext SMB Passwords in Novell Desktop Linux using KDE
loss of business profits or special damages.