

# Password Disclosure for SMB Shares in KDE's Konqueror

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2004-11/0394.html>

---

**From:** Daniel Fabian ([df\\_at\\_sec-consult.com](mailto:df_at_sec-consult.com))

**Date:** 11/29/04

To: [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)

Date: Mon, 29 Nov 2004 09:21:07 +0100

---

| Password Disclosure for SMB Shares in KDE's Konqueror |

---

Date: Nov. 29, 2004

Author: Daniel Fabian

Product: KDE, Konqueror

Vendor: KDE e. V. (<http://www.kde.org>)

Vendor-Status: vendor contacted

Vendor-Patches: none available so far

Attack Vector: Local

~~~~~  
Synopsis

~~~~~  
The KDE program Konqueror allows for browsing SMB shares comfortably through the GUI. By placing a shortcut to an SMB share on KDE's desktop, an attacker can disclose his victim's password in plaintext.

~~~~~  
Affected Versions

~~~~~  
The problem has been successfully reproduced with KDE 3.2.1 on a standard SuSE 9.1 distribution. I have not been able to reproduce the issue on a KDE 3.3.0, however the developers of KDE claimed that there might be a related issue in both KDE 3.3 as well as the upcoming KDE 3.4.

~~~~~  
Vendor Status

~~~~~  
The vendor has been notified and was very cooperative. We set a coordinated disclosure date to Nov. 10th. However Nov. 10th passed, without a patch available. My mail for a new date has gone

## SecurityFocus Bugtraq: Password Disclosure for SMB Shares in KDE's Konqueror

unanswered for more than two weeks now, so I suppose it is ok to release this advisory, very much so since this is not an issue that can be widely exploited anyway.

### ~~~~~ Vulnerability

~~~~~  
Opening the URL "smb:/" in Konqueror allows KDE users to browse the local network for SMB shares. Upon selecting a computer, the user has to enter a password, if access to that computer is restricted. While the URL of the SMB share correctly does not show the password in Konqueror's address bar, this can be easily bypassed by copying a shortcut to a certain share to the desktop.

The created desktop icon will be given a name (and address) following this scheme:

```
smb://domain\username:password@server\sharename
```

The password can be read in plaintext by an attacker. So while a colleague is getting some coffee or having a short nap at his desk, it is most easy to get the password of his open SMB shares.

### ~~~~~ Timeline

~~~~~  
Oct. 06: Discovery of the vulnerability  
Oct. 10: Initial vendor reply  
Nov. 10: Planed coordinated disclosure  
Nov. 29: Final disclosure

### ~~~~~ Counter Measures

~~~~~  
Until a patch is available, just lock your computer every time you leave it (should be done regardless of this issue).

EOF Daniel Fabian / @2004  
d.fabian at sec-consult dot com

### ~~~~~ Contact

~~~~~  
SEC Consult Unternehmensberatung GmbH

Buero Wien  
Blindengasse 3  
A-1080 Wien  
Austria

## SecurityFocus Bugtraq: Password Disclosure for SMB Shares in KDE's Konqueror

Tel.: +43 / 1 / 409 0307 – 570

Fax.: +43 / 1 / 409 0307 – 590

Mail: office at sec-consult dot com

<http://www.sec-consult.com>