

[UNIX] Konqueror Cross Site Scripting Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-09/0038.html>

From: support@securiteam.com

Date: 09/12/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 12 Sep 2002 08:28:02 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

Konqueror Cross Site Scripting Vulnerability

SUMMARY

Konqueror's cross Site scripting protection fails to initialize the domains on sub-(i)frames correctly. As a result, JavaScript can access any foreign subframe that is defined in the HTML source.

DETAILS

Vulnerable systems:

- * KDE version 2.2.2

- * KDE versions 3.0 – 3.0.3

Impact:

Users of Konqueror and other KDE software that uses the KHTML rendering engine may fall victim of a cookie stealing and other cross-site scripting attacks.

Solution:

Apply the appended patch to kdelibs, update to the kdelibs-3.0.3a or, as a workaround, disable JavaScript or cookies.

Securiteam: [UNIX] Konqueror Cross Site Scripting Vulnerability

kdelibs-3.0.3a can be downloaded from:

<<http://download.kde.org/stable/3.0.3>>

<http://download.kde.org/stable/3.0.3> : 02627f595af113f7d544561a7ff6ec85

kdelibs-3.0.3a.tar.bz2

Patch:

A patch for KDE 3.0.3 is available from

<ftp://ftp.kde.org/pub/kde/security_patches>

ftp://ftp.kde.org/pub/kde/security_patches :

523b2fb677310792cbb04861f358d08d post-3.0.3-kdelibs-khtml.diff

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 :

b0b23c3caa062c60375a1160418a2810 post-2.2.2-kdelibs-khtml.diff

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.

-
- **Previous message:** support@securiteam.com: "[EXPL] EFStool Local Root Exploit for Linux/x86"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)