

KDE kdelibs PCX Image Buffer Overflow Vulnerability

By *srlinuxx*

Created *12/04/2005 - 2:54pm*

Submitted by srlinuxx on Tuesday 12th of April 2005 02:54:10 PM Filed under [KDE](#) [1] [Security](#) [2]

Highly Critical

Description:

Bruno Rohee has reported a vulnerability in KDE kdelibs, which potentially can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to an error in the kimgio component when processing PCX image files. This may be exploited via a specially crafted image file to execute arbitrary code via an application linked against the vulnerable library.

The vulnerability has been reported in KDE 3.4.0. Other version may also be affected.

Solution:

Do not open untrusted images in applications linked against the vulnerable library.

[Source](#) [3]

[KDE Security](#)

Source URL: <http://www.tuxmachines.org/node/580>

Links:

[1] <http://www.tuxmachines.org/taxonomy/term/108>

[2] <http://www.tuxmachines.org/taxonomy/term/59>

[3] <http://secunia.com/advisories/14908/>