

[UNIX] Multiple Vulnerabilities in KDE (command shell)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-12/0096.html>

From: support@securiteam.com

Date: 12/26/02

From: support@securiteam.com

To: list@securiteam.com

Date: 26 Dec 2002 23:37:38 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

Multiple Vulnerabilities in KDE (command shell)

SUMMARY

In some instances KDE fails to properly quote parameters of instructions passed to a command shell for execution.

These parameters may incorporate data such as URLs, filenames and e-mail addresses, and this data may be provided remotely to a victim in an e-mail, a webpage or files on a network file system or other untrusted source.

By carefully crafting such data an attacker might be able to execute arbitrary commands on a vulnerable system using the victim's account and privileges.

The KDE Project is aware of several possible ways to exploit these vulnerabilities and is releasing this advisory with patches to correct the issues. The patches also provide better safe guards and check data from untrusted sources more strictly in multiple places.

DETAILS

Securiteam: [UNIX] Multiple Vulnerabilities in KDE (command shell)

Vulnerable systems:

* All KDE 2 releases and all KDE 3 releases (up to and including KDE 3.0.5).

Impact:

The vulnerabilities potentially enable local or remote attackers to compromise the privacy of a victim's data and to execute arbitrary shell commands with the victim's privileges, such as erasing files or accessing or modifying data.

Solution:

The code audit resulted in several fixes which have been applied to the KDE 2.2.x and each KDE 3.x branch.

All identified problems have been corrected in KDE 3.0.5a. For affected KDE 3.0 systems, we strongly recommend upgrading to this latest stable release.

KDE 3.0.5a can be downloaded from:

<http://download.kde.org/stable/3.0.5a/>

<http://download.kde.org/stable/3.0.5a/>

Please visit the 3.0.5a Info Page (<http://www.kde.org/info/3.0.5a.html>) and your vendor's website for exact package locations and information about available binary packages or updates.

For affected KDE 2 systems, a patch for the 2.2.2 source code has been made available which fixes these vulnerabilities. Contact your OS vendor / binary package provider for information about how to obtain updated binary packages.

Patches:

Patches are available for KDE 2.2.2 from the KDE FTP server (

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

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

MD5SUM PATCH

```
522331e2b47f84956eb2df1fcf89ba17 post-2.2.2-kdebase.diff
0dbd747882b942465646efe0ba6af802 post-2.2.2-kdegames.diff
4b9c93acd452d1de2f4f0bca5b05593f post-2.2.2-kdegraphics.diff
93a12594d0fb48c7b50bfd4a10a9935d post-2.2.2-kdelibs.diff
d1d25b39ee98e340ac3730f7afe54f0c post-2.2.2-kdemultimedia.diff
59ac7be4995bed8b119a4e5882e54cff post-2.2.2-kdenetwork.diff
0a3ae9eeceefb2f631a26ec787663a9 post-2.2.2-kdepim.diff
690c7fdab1bbc743eafac9b06997a03b post-2.2.2-kdesdk.diff
8174e328f47e18a8a52b13b34f5c54e5 post-2.2.2-kdeutils.diff
```

Timeline and credits:

11/26/2002 FozZy of the "Hackademy Audit Project" notified the

Securiteam: [UNIX] Multiple Vulnerabilities in KDE (command shell)

<<mailto:security@kde.org>> KDE Security Team about vulnerable code parts.

11/27/2002 Patches for the initially reported vulnerabilities were applied to KDE CVS.

11/27/2002 An audit of KDE CVS was started to find more instances of the problematic code sequences.

12/06/2002 KDE 3.1 release was delayed because the audit was not yet finished.

12/17/2002 Patches for KDE 2.2.2 were created.

12/20/2002 KDE 3.0.5a tar balls were generated and released.

12/21/2002 Public Security Advisory by the KDE Security team.

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.