

# [UNIX] KDE PS/PDF handling vulnerability

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-04/0019.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 04/14/03

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 14 Apr 2003 16:49:15 +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

In the US?

Contact Beyond Security at our new California office  
housewarming rates on automated network vulnerability  
scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or [ussales@beyondsecurity.com](mailto:ussales@beyondsecurity.com)

-----

KDE PS/PDF handling vulnerability

---

## SUMMARY

KDE uses Ghostscript for processing of PostScript (PS) and PDF files in a way that allows for the execution of arbitrary commands that can be contained in such files.

## DETAILS

An attacker can prepare a malicious PostScript or PDF file which will provide the attacker with access to the victim's account and privileges when the victim opens this malicious file for viewing or when the victim browses a directory containing such malicious file and has file previews enabled.

An attacker can provide malicious files remotely to a victim in an e-mail, as part of a webpage, via an ftp server and possible other means.

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

Securiteam: [UNIX] KDE PS/PDF handling vulnerability

or modifying data.

Effected versions:

All KDE 2 and KDE 3 versions up to and including KDE 3.1.1.

Solution:

The affected applications have been fixed in KDE 3.0.5b and KDE 3.1.1a, both released today. We strongly recommend upgrading to these releases.

Upgrading KDEGraphics package and associated to stable version 2.2.2-6.11 also fixes the problem.

ADDITIONAL INFORMATION

The original article can be found at:

<<http://www.kde.org/info/security/advisory-20030409-1.txt>>  
<http://www.kde.org/info/security/advisory-20030409-1.txt>

=====

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](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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.