

[UNIX] KOffice PDF Import Filter Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0090.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/23/05

To: list@securiteam.com

Date: 23 Jan 2005 14:34:19 +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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

KOffice PDF Import Filter Vulnerability

SUMMARY

The KOffice PDF Import Filter shares code with xpdf. xpdf contains a buffer overflow that can be triggered by a specially crafted PDF file.

DETAILS

Vulnerable Systems:

* KOffice version 1.3 up to including KOffice version 1.3.5

Impact:

Remotely supplied pdf files can be used to execute arbitrary code on the client machine when the user opens such file in KOffice.

Solution:

Source code patches have been made available which fix these vulnerabilities. Contact your OS vendor / binary package provider for information about how to obtain updated binary packages.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0064>>
CAN-2005-0064

Securiteam: [UNIX] KOffice PDF Import Filter Vulnerability

Patch:

Patch for KOffice 1.3.5 is available from
<ftp://ftp.kde.org/pub/kde/security_patches>
ftp://ftp.kde.org/pub/kde/security_patches.

Time line and credits:

19/01/2005 KDE Security Team alerted by Carsten Lohrke
19/01/2005 Patches from xpdf 3.00pl3 applied to KDE CVS and patches prepared
20/01/2005 Public disclosure

ADDITIONAL INFORMATION

The information has been provided by <<mailto:bastian@kde.org>> Waldo Bastian.

The original article can be found at:
<<http://www.kde.org/info/security/advisory-20050120-1.txt>>
<http://www.kde.org/info/security/advisory-20050120-1.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
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.