

# [UNIX] Multiple UNIX/Linux Vendor Xpdf makeFileKey2 Stack Overflow

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0087.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 01/23/05

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

Date: 23 Jan 2005 14:38:37 +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>

-----

Multiple UNIX/Linux Vendor Xpdf makeFileKey2 Stack Overflow

---

## SUMMARY

<<http://www.foolabs.com/xpdf/>> Xpdf is an open-source viewer for PDF files.

Remote exploitation of a buffer overflow vulnerability in the xpdf PDF viewer included in multiple UNIX and Linux distributions could allow for arbitrary code execution as the user viewing a PDF file.

## DETAILS

Vulnerable Systems:

- \* Xpdf Version 3.00 and prior

Immune Systems:

- \* Xpdf Version 3.00p13 or newer

The vulnerability specifically exists due to insufficient bounds checking while processing a PDF file that provides malicious values in the /Encrypt /Length tag.

## Securiteam: [UNIX] Multiple UNIX/Linux Vendor Xpdf makeFileKey2 Stack Overflow

### Vulnerable Code:

The offending code can be found in the Decrypt::makeFileKey2 function in the source file xpdf/Decrypt.cc.

```
GBool Decrypt::makeFileKey2(int encVersion, int encRevision,
                           int keyLength, GString *ownerKey,
                           GString *userKey, int permissions,
                           GString *fileID, String *userPassword,
                           Guchar *fileKey) {
    Guchar *buf;
    Guchar test[32];
    Guchar fState[256];
    Guchar tmpKey[16];
    Guchar fx, fy;
    int len, i, j;
    GBool ok;
    ...

    memcpy(test, userKey->getCString(), 32);
    for (i = 19; i >= 0; --i) {
        for (j = 0; j < keyLength; ++j) {
[overflow] tmpKey[j] = fileKey[j] ^ i;
        }
        ...
    }
    ...
}
```

In this piece of code, the keyLength value is ultimately supplied by the PDF file. This allows an attacker to specify an arbitrarily large value and overwrite portions of stack memory. As a consequence, arbitrary code execution is possible.

Successful exploitation of this vulnerability leads to arbitrary code execution as the user who opened the malicious file. An attacker would have to convince a target to open the provided file in order to exploit this vulnerability, thus lessening the impact. Exploitation can be performed reliably, especially with knowledge of the target system.

### Vendor Status:

A patch to address this issue is available at:

<<ftp://ftp.foolabs.com/pub/xpdf/xpdf-3.00pl3.patch>>

<ftp://ftp.foolabs.com/pub/xpdf/xpdf-3.00pl3.patch>

Updated binaries (ver. 3.00pl3) to address this issue are available at:

<<http://www.foolabs.com/xpdf/download.html>>

<http://www.foolabs.com/xpdf/download.html>

### Disclosure Timeline:

01/06/2005 – Initial vendor notification

01/12/2005 – Initial vendor response

01/18/2005 – Coordinated public disclosure

Securiteam: [UNIX] Multiple UNIX/Linux Vendor Xpdf makeFileKey2 Stack Overflow

CVE Information:

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

ADDITIONAL INFORMATION

The information has been provided by  
<<mailto:idlabs-advisories@idefense.com>> iDEFENSE.

The original article can be found at:  
<[www.idefense.com/application/poi/display?id=186&type=vulnerabilities](http://www.idefense.com/application/poi/display?id=186&type=vulnerabilities)>  
[www.idefense.com/application/poi/display?id=186&type=vulnerabilities](http://www.idefense.com/application/poi/display?id=186&type=vulnerabilities)

=====

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.