

# [VulnWatch] iDEFENSE Security Advisory 12.21.04: Multiple Vendor xpdf PDF Viewer Buffer Overflow Vulnerability

**Source:** <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2004-12/0019.html>

---

**From:** customer service mailbox ([customerservice\\_at\\_idefense.com](mailto:customerservice_at_idefense.com))

**Date:** 12/21/04

Date: Tue, 21 Dec 2004 17:37:03 -0500

To: <[vulnwatch@vulnwatch.org](mailto:vulnwatch@vulnwatch.org)>

Multiple Vendor xpdf PDF Viewer Buffer Overflow Vulnerability

iDEFENSE Security Advisory 12.21.04

[www.idefense.com/application/poi/display?id=172&type=vulnerabilities](http://www.idefense.com/application/poi/display?id=172&type=vulnerabilities)

December 21, 2004

## I. BACKGROUND

Xpdf is an open-source viewer for Portable Document Format (PDF) files.

## II. DESCRIPTION

Remote exploitation of a buffer overflow vulnerability in the xpdf PDF viewer, as included in multiple Linux distributions, could allow attackers to execute arbitrary code as the user viewing a PDF file. The offending code can be found in the `Gfx::doImage()` function in the source

file `xpdf/Gfx.cc`.

```
void Gfx::doImage(Object *ref, Stream *str, GBool inlineImg) {
    Dict *dict;
    int width, height;
    int bits;
    GBool mask;
    GBool invert;
    GfxColorSpace *colorSpace;
    GfxImageColorMap *colorMap;
    Object maskObj;
    GBool haveMask;
    int maskColors[2*gfxColorMaxComps];
    Object obj1, obj2;
    int i;
```

```
...
// get the mask
haveMask = gFalse;
dict->lookup("Mask", &maskObj);
if (maskObj.isArray()) {
    for (i = 0; i < maskObj.arrayGetLength(); ++i) {
        maskObj.arrayGet(i, &obj1);
[!] maskColors[i] = obj1.getInt();
        obj1.free();
    }
    haveMask = gTrue;
}
...
}
```

Due to the fact that the loop boundaries are not less than the storage area, the maskColors array is eventually filled up. After that, local variables and other stack memory is overwritten. This ultimately leads to control of program flow and arbitrary code execution.

### III. ANALYSIS

The severity of this issue is mitigated by the fact that several of the local overwritten variables in doImage() are referenced prior to EIP being restored; therefore, before the attack gains control of the target

process. However, an attacker with knowledge of the remote operating system can construct and validate a malicious payload before attempting exploitation, thus increasing the chances of success. An attacker must convince a target user to open the malicious file to exploit this vulnerability.

### IV. DETECTION

iDEFENSE has confirmed the existence of this vulnerability in version 3.00 of xpdf. It is suspected previous versions are also vulnerable.

The following vendors included vulnerable xpdf packages:

- Novell SUSE
- Red Hat, Inc.
- Fedora Project
- Debian Project
- Gentoo Foundation
- FreeBSD Project (ports)
- OpenBSD

### V. WORKAROUND

Only open PDF files from trusted individuals.

## VI. VENDOR RESPONSE

A patch to address this vulnerability is available from:

[ftp://ftp.foolabs.com/pub/xpdf/xpdf-3.00p12\\_patch](ftp://ftp.foolabs.com/pub/xpdf/xpdf-3.00p12_patch)

Updated binaries (version 3.00p12) are available from:

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

## VII. CVE INFORMATION

The Common Vulnerabilities and Exposures (CVE) project has assigned the names CAN-2004-1125 to these issues. This is a candidate for inclusion in the CVE list (<http://cve.mitre.org>), which standardizes names for security problems.

## VIII. DISCLOSURE TIMELINE

11/23/2004 Initial vendor notification

11/29/2004 Initial vendor response

12/21/2004 Coordinated public disclosure

## IX. CREDIT

The discoverer of this vulnerability wishes to remain anonymous.

Get paid for vulnerability research

<http://www.idefense.com/poi/teams/vcp.jsp>

## X. LEGAL NOTICES

Copyright (c) 2004 iDEFENSE, Inc.

Permission is granted for the redistribution of this alert electronically. It may not be edited in any way without the express written consent of iDEFENSE. If you wish to reprint the whole or any part of this alert in any other medium other than electronically, please email [customerservice@idefense.com](mailto:customerservice@idefense.com) for permission.

Disclaimer: The information in the advisory is believed to be accurate at the time of publishing based on currently available information. Use of the information constitutes acceptance for use in an AS IS condition. There are no warranties with regard to this information. Neither the author nor the publisher accepts any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.