

# [UNIX] Multiple Vendor X Server fonts.dir File Parsing Integer Overflow Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-04/msg00007.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxxx)>
  - *Date:* 4 Apr 2007 17:39:54 +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 Vendor X Server fonts.dir File Parsing Integer Overflow  
Vulnerability

---

## SUMMARY

The X Window System (or X11) is "a graphical windowing system used on Unix-like systems. It is based on a client/server model". Local exploitation of an integer overflow vulnerability in multiple vendors' implementations of the X Window System font information file parsing component could allow execution of arbitrary commands with elevated privileges.

## DETAILS

Vulnerable Systems:  
\* in X.Org X11R7.1

Immune Systems:  
\* in X.Org X11R7.2

The vulnerability specifically exists in the parsing of the "fonts.dir" font information file. When the element count on the first line of the file specifies it contains more than 1,073,741,824 (2 to the power of 30)

## [UNIX] Multiple Vendor X Server fonts.dir File Parsing Integer Overflow Vulnerability

elements, a potentially exploitable heap overflow condition occurs.

### Analysis:

Exploitation allows attackers to execute arbitrary code with elevated privileges.

As the X11 server requires direct access to video hardware, it runs with elevated privileges. A user compromising an X server would gain those permissions.

In order to exploit this vulnerability, an attacker would need to be able to cause the X server to use a maliciously constructed font. The X11 server contains multiple methods for a user to define additional paths to look for fonts. An exploit has been developed using the "-fp" command line option to the X11 server to pass the location of the attack to the server. It is also possible to use "xset" command with the "fp" option to perform an attack on an already running server.

Some distributions allow users to start the X11 server only if they are logged on at the console, while others will allow any user to start it.

Attempts at exploiting this vulnerability may put the console into an unusable state. This will not prevent repeated exploitation attempts.

### Workaround:

iDefense is currently unaware of any effective workaround for this issue.

### Vendor response:

The X.Org Foundation has addressed this vulnerability with source code patches. More information can be found from their advisory at the following URL.

<<http://lists.freedesktop.org/archives/xorg-announce/2007-April/000286.html>>  
<http://lists.freedesktop.org/archives/xorg-announce/2007-April/000286.html>

### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1352>>  
CVE-2007-1352

### Disclosure Timeline:

02/21/2007 – Initial vendor notification  
02/21/2007 – Initial vendor response  
04/03/2007 – Coordinated public disclosure

## ADDITIONAL INFORMATION

The information has been provided by Greg MacManus of iDefense Labs.

The original article can be found at:

<<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=502>>  
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=502>

=====

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@xxxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====

=====

**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.