

# [UNIX] Remote and Local Vulnerabilities In XFree86 Font Libraries

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-09/0001.html>

---

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

*Date:* 09/02/03

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

Date: 2 Sep 2003 15:05:44 +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>

-----

Remote and Local Vulnerabilities In XFree86 Font Libraries

---

## SUMMARY

<<http://xfree86.org>> Xfree86 is "a freely redistributable open-source implementation of the X Window System. XFree86 runs primarily on UNIX® and UNIX-like operating systems such as Linux, all of the BSD variants, Sun Solaris x86, Mac OS X (via Darwin), as well as other platforms like OS/2 and Cygwin".

Several bugs exist in the font libraries of XFree86 font libraries. These bugs could potentially lead to the execution of arbitrary code by a remote user in any process that calls the functions in question. The functions are related to the transfer and enumeration of fonts from font servers to clients, limiting the range of the exposure caused by these bugs.

## DETAILS

Vulnerable Systems:

- \* XFree86 4.3.0

Immune Systems:

- \* XFree86 4.3.0.1 (latest CVS)

## Securiteam: [UNIX] Remote and Local Vulnerabilities In XFree86 Font Libraries

Several variables that are passed from a font server to a client are not adequately checked, allowing integer overflows to cause erroneous sizes of buffers to be calculated. These erroneous calculations can lead to buffers on the heap and stack overflowing, potentially leading to arbitrary code execution. As stated before, the risk is limited by the fact that only clients can be affected remotely by these bugs, but in some (non default) configurations, both xfs and XServer can act as clients to remote font servers. In these configurations, both xfs and XServer could be potentially compromised remotely. In addition, it is possible for a local unprivileged user to alter the configuration of XServer in such a manner as to force it to load a font from an arbitrary font server. Since XServer is setuid root by default, a local user may potentially gain root privileges.

### Workaround:

\* To prevent the local privilege escalation, remove the suid bit from the XServer binary:

```
chmod u-s XFree86
```

\* Ensure xfs and XServer do not include untrusted font servers in their font search paths.

### Fix:

The current CVS version of XFree86 has been updated to correct these issues.

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:blexim@hush.com>> blexim of isen

=====

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.