[UNIX] Multiple Vendor X Font Server Multiple Vulnerabilities

Source: http://www.derkeiler.com/Mailing−Lists/Securiteam/2007−10/msg00008.html

- *From*: SecuriTeam <support@xxxxxxxxxxxxxx>
- *Date*: 8 Oct 2007 19:16:38 +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/mailinglist.html

− − − − − − − − −

Multiple Vendor X Font Server Multiple Vulnerabilities
−−−

to an improperly sized memory allocation. This results in a heap overflow.

Additionally, a heap corruption vulnerability exists within the handlers for the QueryXBitmaps and QueryXExtents protocol requests. Both requests result in a call to the swap_char2b() function. This function takes a 32bit integer from the request, and uses it as the number of bytes to swap in the request buffer. This allows an attacker to swap an arbitrary number of bytes on the heap.

Exploitation of these vulnerabilities could result in the execution of arbitrary code with the privileges of the X Font Server, usually 'xfs'.

On current versions of Solaris, these vulnerabilities are remotely exploitable. The XFS service is turned on by default, and listens on TCP port 7100. On modern Linux systems, these vulnerabilities are only locally exploitable since the server is configured to listen on a UNIX socket only.

Workaround:
On Solaris, stop XFS from listening remotely by disabling it via the service manager.

Vendor Status:
The X.Org team has addressed these vulnerabilities with the release of XFS version 1.0.5. Additionally, a patch for version 1.0.4 has been made available. For more information, consult the X.Org advisory at the following URL:

<http://lists.freedesktop.org/archives/xorg−announce/2007−October/000416.html>
http://lists.freedesktop.org/archives/xorg−announce/2007−October/000416.html

CVE Information:
<http://www.cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2007−4568>
CVE−2007−4568

Disclosure Timeline:
* 09/05/2007 − Initial vendor notification
* 09/08/2007 − Initial vendor response
* 10/02/2007 − Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by iDefense.
The original article can be found at:

<http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=602>
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=602

==========

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@xxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list−subscribe@xxxxxxxxxxxxxx

==========
==========

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.