

[UNIX] Multiple Vendor X Server Vulnerabilities (XFree86-Misc, EVI, MIT-SHM, TOG-CUP, XInput)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-01/msg00041.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 20 Jan 2008 13:22:07 +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 Vulnerabilities (XFree86-Misc, EVI, MIT-SHM, TOG-CUP, XInput)

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". Multiple vulnerabilities have been discovered in the X Server product, these vulnerabilities allow local users to gain elevated privileges by exploiting security issues found in the product.

DETAILS

Vulnerable Systems:

- * X.org X11 version R7.3

Immune Systems:

- * Xserver version 1.4.1

Multiple Vendor X Server XFree86-Misc Extension Invalid Array Index Vulnerability

Local exploitation of an invalid array index vulnerability in the X.Org X server, as included in various vendors' operating system distributions,

[UNIX] Multiple Vendor X Server Vulnerabilities (XFree86-Misc, EVI, MIT-SHM, TOG-CUP, XInput)

could allow an attacker to execute arbitrary code with the privileges of the X server, typically root.

The vulnerability exists within the XFree86-Misc extension. When processing a request, a 32-bit value from the client's request is used as an index into an array of structures. This structure contains an array of function pointers, one of which is used later in the request handling. By supplying a large array index, an arbitrary function pointer can be dereferenced. This results in the execution of arbitrary code.

Analysis:

Exploitation allows an attacker to execute arbitrary code with root privileges. In order to exploit this vulnerability, an attacker must be able to send commands to an affected X server. This typically requires access to the console or access to the same account as a user who is on the console.

If an X Server is configured to listen for TCP based client connections, and a client is granted access to create sessions (via the xhosts file), then the vulnerability can be exploited remotely.

Workaround:

If the XFree86-Misc extension has not been built-in to the server, then it can be prevented from loading by inserting the following into the X configuration file (usually in /etc/X11/xorg.conf).

```
Section "Module"  
SubSection "extmod"  
Option "omit XFree86-Misc"  
EndSubSection  
EndSection
```

To check if the extension is built-in to the server, grep the output of the X Server log file.

```
grep built-in /var/log/Xorg.0.log
```

The result will list all built in extensions. The location of the log file may need to be changed.

Vendor response:

The X.Org team has addressed this vulnerability with the release of Xserver version 1.4.1. Additionally, patches for versions 1.4 and 1.2 have been made available. For more information, consult the X.Org advisory at the following URL.

<<http://lists.freedesktop.org/archives/xorg/2008-January/031918.html>>
<http://lists.freedesktop.org/archives/xorg/2008-January/031918.html>

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5760>>
CVE-2007-5760

Disclosure Timeline:

11/29/2007 – Initial vendor response

11/30/2007 – Initial vendor notification

01/17/2008 – Coordinated public disclosure

Multiple Vendor X Server EVI and MIT-SHM Extensions Integer Overflow Vulnerabilities

Local exploitation of multiple integer overflow vulnerabilities in the X.Org X server, as included in various vendors' operating system distributions, could allow an attacker to execute arbitrary code with the privileges of the X server, typically root.

One vulnerability exists within the EVI extension. When processing a request, the server uses a 32-bit value provided by the client in an arithmetic operation that calculates the number of bytes to allocate for a dynamic buffer. This operation can overflow, which later leads to a potentially exploitable heap overflow.

Another vulnerability exists within the MIT-SHM extension. When allocating a pixmap, the server uses values from the request to verify that the requested size is not greater than the amount of allocated shared memory. The calculation can overflow, which leads to the overwriting of arbitrary addresses in memory that aren't part of the shared memory segment.

Analysis:

Exploitation allows an attacker to execute arbitrary code with root privileges. In order to exploit these vulnerabilities, an attacker must be able to send commands to an affected X server. This typically requires access to the console or access to the same account as a user who is on the console.

If an X Server is configured to listen for TCP based client connections, and a client is granted access to create sessions (via the xhosts file), then these vulnerabilities can be exploited remotely.

Workaround:

If the EVI or MIT-SHM extensions have not been built-in to the server, they can be prevented from loading by inserting the following into the X configuration file (usually in /etc/X11/xorg.conf).

```
Section "Module"  
SubSection "extmod"  
Option "omit Extended-Visual-Information"  
Option "omit MIT-SHM"  
EndSubSection  
EndSection
```

To check if an extension is built-in to the server, grep the output of the X Server log file.

```
grep built-in /var/log/Xorg.0.log
```

[UNIX] Multiple Vendor X Server Vulnerabilities (XFree86-Misc, EVI, MIT-SHM, TOG-CUP, XInput)

The result will list all built in extensions. The location of the log file may need to be changed.

Vendor response:

The X.Org team has addressed these vulnerabilities with the release of Xserver version 1.4.1. Additionally, patches for versions 1.4 and 1.2 have been made available. For more information, consult the X.Org advisory at the following URL.

<<http://lists.freedesktop.org/archives/xorg/2008-January/031918.html>>
<http://lists.freedesktop.org/archives/xorg/2008-January/031918.html>

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6429>>
CVE-2007-6429

Disclosure Timeline:

11/29/2007 – Initial vendor notification
11/29/2007 – Initial vendor response
01/17/2008 – Coordinated public disclosure

Multiple Vendor X Server TOG-CUP Extension Information Disclosure Vulnerability

Local exploitation of an information disclosure vulnerability in the X.Org X server, as included in various vendors' operating system distributions, could allow an attacker to gain access to sensitive information stored in server memory.

The vulnerable code exists within the TOG-CUP extension. A 32-bit client supplied value is taken directly from the request, and then used as an index into an array. The value located at this index is then stored into a buffer which is later sent to the client. This allows a client to read memory from arbitrary locations in server memory.

Analysis:

Exploitation allows an attacker to read arbitrary memory within the X Server's address space.

By itself, the impact of this vulnerability is minimal. However, when coupled with a code execution vulnerability, this vulnerability can be used to greatly increase the reliability of an exploit.

If an X Server is configured to listen for TCP based client connections, and a client is granted access to create sessions (via the xhosts file), then the vulnerability can be exploited remotely.

Workaround:

If the TOG-CUP extension has not been built-in to the server, then it can be prevented from loading by inserting the following into the X configuration file (usually in /etc/X11/xorg.conf).

Section "Module"

```
SubSection "extmod"  
Option "omit TOG-CUP"  
EndSubSection  
EndSection
```

To check if the extension is built-in to the server, grep the output of the X Server log file as shown below.

```
grep built-in /var/log/Xorg.0.log
```

The result will list all built in extensions. The location of the log file may need to be changed.

Vendor response:

The X.Org team has addressed this vulnerability with the release of Xserver version 1.4.1. Additionally, patches for versions 1.4 and 1.2 have been made available. For more information, consult the X.Org advisory at the following URL.

<<http://lists.freedesktop.org/archives/xorg/2008-January/031918.html>>

<http://lists.freedesktop.org/archives/xorg/2008-January/031918.html>

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6428>>

CVE-2007-6428

Disclosure Timeline:

11/29/2007 – Initial vendor notification

12/13/2007 – Initial vendor response

01/17/2008 – Coordinated public disclosure

Multiple Vendor X Server XInput Extension Multiple Memory Corruption Vulnerabilities

Local exploitation of multiple memory corruption vulnerabilities in the X.Org X server, as included in various vendors' operating system distributions, allows attackers to execute arbitrary code with the privileges of the X server, typically root.

Vulnerable code exists within multiple functions in the XInput extension. By sending specially crafted X11 requests, an attacker is able to corrupt heap memory located after their request data. This results in a potentially exploitable condition.

Analysis:

Exploitation allows an attacker to execute arbitrary code with root privileges. In order to exploit these vulnerabilities, an attacker must be able to send commands to an affected X server. This typically requires access to the console or access to the same account as a user who is on the console.

If an X Server is configured to listen for TCP based client connections, and a client is granted access to create sessions (via the xhosts file), then these vulnerabilities can be exploited remotely.

Vendor response:

The X.Org team has addressed these vulnerabilities with the release of Xserver version 1.4.1. Additionally, patches for versions 1.4 and 1.2 have been made available. For more information, consult the X.Org advisory at the following URL.

<<http://lists.freedesktop.org/archives/xorg/2008-January/031918.html>>
<http://lists.freedesktop.org/archives/xorg/2008-January/031918.html>

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6427>>
CVE-2007-6427

Disclosure Timeline:

11/29/2007 – Initial vendor notification
12/04/2007 – Initial vendor response
01/17/2008 – Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by iDefense Labs.

The original article can be found at:

<<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=646>>
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=646>,
<<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=645>>
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=645>,
<<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=644>>
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=644>
and
<<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=643>>
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=643>

=====

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@xxxxxxxxxxxxxxxx

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

=====
=====

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.