

# [NEWS] GTK+ gdk-pixbuf XPM Loader Heap Overflow

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00031.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 11 Dec 2005 11:36:14 +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>

-----

GTK+ gdk-pixbuf XPM Loader Heap Overflow

---

## SUMMARY

" <<http://www.gtk.org/>> GTK+ is a multi-platform toolkit for creating graphical user interfaces. Offering a complete set of widgets, GTK+ is suitable for projects ranging from small one-off projects to complete application suites."

Remote exploitation of heap overflow vulnerability in implementations of the GTK+ gdk-pixbuf XPM image rendering library allow attackers to execute arbitrary code.

## DETAILS

Vulnerable Systems:

\* gtk+ 2.4.0

The vulnerability specifically exists due to an integer overflow while processing XPM files. The following code snippet illustrates the vulnerability:

```
if (n_col <= 0 || n_col >= G_MAXINT / (cpp + 1)) {
```

## [NEWS] GTK+ gdk-pixbuf XPM Loader Heap Overflow

```
g_set_error (error,  
GDK_PIXBUF_ERROR,  
GDK_PIXBUF_ERROR_CORRUPT_IMAGE,  
_("XPM file has invalid number of colors"));  
return NULL;  
}  
[...]  
colors = (XPMColor *) g_try_malloc ((sizeof (XPMColor) * n_col));  
[...]
```

The validity check of `n_col` is enough to prevent an integer overflow in the first `g_try_malloc`, however there is not a proper check for the second `g_try_malloc`, which allows an undersized heap buffer to be allocated, then overflowed while using `n_col` as an upper bounds in a copying loop. This can be used to execute arbitrary code via traditional heap overflow 4 byte write methods or by overwriting adjacent areas of the heap with important values such as function pointers.

Exploitation allow for arbitrary code execution in the context of the user running the affected application. As this library is used in a variety of applications, this vulnerability could be exploited either remotely, via a networked application or locally.

### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3186>>  
CAN-2005-3186

### Disclosure Timeline:

10/12/2005 Initial vendor notification  
10/14/2005 Initial vendor response  
11/15/2005 Coordinated public disclosure

### ADDITIONAL INFORMATION

The information has been provided by

<<mailto:idlabs-advisories@xxxxxxxxxxxxxxxxxxxx>> iDEFENSE Labs.

The original article can be found at:

<<http://www.idefense.com/application/poi/display?id=339&type=vulnerabilities&flashstatus=true>>  
<http://www.idefense.com/application/poi/display?id=339&type=vulnerabilities&flashstatus=true>

=====

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](mailto:list-unsubscribe@xxxxxxxxxxxxxxxx)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@xxxxxxxxxxxxxxxx](mailto: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.

- 
- Prev by Date: [\*\[UNIX\] Ethereal OSPF Protocol Dissector Buffer Overflow\*](#)
  - Next by Date: [\*\[TOOL\] MS SQL Server Captured Authentication Packets Cracker\*](#)
  - Previous by thread: [\*\[UNIX\] Ethereal OSPF Protocol Dissector Buffer Overflow\*](#)
  - Next by thread: [\*\[TOOL\] MS SQL Server Captured Authentication Packets Cracker\*](#)
  - Index(es):
    - ◆ [\*Date\*](#)
    - ◆ [\*Thread\*](#)