

# [UNIX] GTK+ XPM Decoder Parsing Overflows

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-09/0051.html>

---

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

**Date:** 09/21/04

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

Date: 21 Sep 2004 13:57:33 +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+ XPM Decoder Parsing Overflows

---

## 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."

Two parsing flaws have been found in the XPM parser within the GTK+ library, one leading to a heap-based overflow and another to a classic stack-based overflow condition.

## DETAILS

### Vulnerable Systems:

- \* The GIMP Toolkit (GTK+) version 2.4.4, possibly prior

### Immune Systems:

- \* The GIMP Toolkit (GTK+) version 2.4.10

### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0782>>

CAN-2004-0782

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0783>>

## Securiteam: [UNIX] GTK+ XPM Decoder Parsing Overflows

CAN-2004-0783

The first vulnerability, labeled CAN-2004-0782, is a heap-based overflow in the `pixbuf_create_from_xpm()` function (`io-xpm.c`). The small relevant piece of code is:

```
name_buf = g_new (gchar, n_col * (cpp + 1));
colors = g_new (XPMColor, n_col);
```

The `n_col` variable is an arbitrary integer value taken directly from the XPM file, while `cpp` is an integer ranging from 1 to 31, also taken from the XPM image file. By careful choice of values of `n_col` and `cpp`, integer overflow can occur on integer multiplication. This leads to heap buffers being allocated that cannot hold `n_col` elements, so a subsequent heap overflow occurs.

An example proof of concept XPM image can be downloaded from <http://scary.beasts.org/misc/gdk1.xpm>

The second overflow, labeled CAN-2004-0783, is a subtle bug found in the `xpm_extract_color()` function (`io-xpm.c`). The following code section illustrates the problem:

```
gint space = 128;
gchar word[128], color[128], current_color[128];
..
    if (color[0] != '\0') {
        strcat (color, " ");
[*] space--;
    }
    strncat (color, word, space);
    space -= MIN (space, strlen (word));
```

An actual attempt is made to prevent a stack based overflow in this case. However, due to a logic problem it is still possible to overflow under a certain condition. When "space" reaches 0, "space" can be sent to -1 by the line marked with `[*]`, if the color string is broken up by whitespace. When "space" is -1, the `strncat()` call is effectively morphed to a `strcat()` call, allowing overflow of the "color" buffer. The data will overflow into the "word" buffer which poses a minor inconvenience in exploitation. However, minor it is.

An example proof of concept XPM image demonstrating this issue can be obtained from <http://scary.beasts.org/misc/gdk2.xpm>

### ADDITIONAL INFORMATION

The information has been provided by <mailto:chris@scary.beasts.org>  
Chris Evans.

The original article can be found at:

<http://scary.beasts.org/security/CESA-2004-005.txt>

Securiteam: [UNIX] GTK+ XPM Decoder Parsing Overflows

<http://scary.beasts.org/security/CESA-2004-005.txt>

=====

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.