

[UNIX] Gttdiskfree Insecure Temporary File Creation

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-09/0065.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 09/15/05

To: list@securiteam.com

Date: 15 Sep 2005 11:54:25 +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>

Gttdiskfree Insecure Temporary File Creation

SUMMARY

"gttdiskfree – A Gnome program which shows free and used space on your filesystems."

Improper use of temporary files allows local attackers to perform a symbolic link attack and execute programs with elevated privileges using gttdiskfree.

DETAILS

Vulnerable Systems:

* gttdiskfree version 1.9.3 and prior

gttdiskfree creates a statically named temporary file of '/tmp/gttdiskfree'.

Attackers may perform a symbolic link attack and execute programs with elevated privileges.

Vulnerable code:

Securiteam: [UNIX] Gttdiskfree Insecure Temporary File Creation

```
src/mount.h
23 #define TUBE_NAME "/tmp/gttdiskfree"

src/mount.c
32 open_cmd_tube (const gchar *cmd, const gchar *mount_point)
33 {
34     gint status;
35     gchar error[MAXLINE], *line;
36     FILE *sh, *tmp;
37
38     setbuf(stdout, error);
39     line = g_strconcat(cmd, " ", mount_point, " &> ", TUBE_NAME,
NULL);
40     sh = popen(line, "r");
41     g_free(line);
42
43     status = pclose(sh);
44
45     if (status == 0) {
46         remove(TUBE_NAME);
47         gui_list_main_update(GTK_TREE_VIEW(list_treeview));
48
49         return;
50     } else {
51         if ((tmp = fopen(TUBE_NAME, "r")) == NULL) {
52             gui_list_main_update(GTK_TREE_VIEW(list_treeview));
53
54             return;
55         }
56         if (fgets(error, MAXLINE-1, tmp) == NULL) {
57             fclose(tmp);
58             remove(TUBE_NAME);
59
60             gui_list_main_update(GTK_TREE_VIEW(list_treeview));
61             return;
62         }
63         fclose(tmp);
64         remove(TUBE_NAME);
65         error_window(error);
66     }
67     gui_list_main_update(GTK_TREE_VIEW(list_treeview));
68
69     return;
70 }
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:exploits@zataz.net>> ZATAZ Audits.

The original article can be found at:

Securiteam: [UNIX] Gtkdiskfree Insecure Temporary File Creation

<<http://www.zataz.net/adviso/gtkdiskfree-09052005.txt>>
<http://www.zataz.net/adviso/gtkdiskfree-09052005.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

In order to subscribe to the mailing list, simply forward this email to: 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.