

# [UNIX] GNOME Foundation Display Manager gdmchooser Format String Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-12/msg00021.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 19 Dec 2006 10:35:47 +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>

-----

GNOME Foundation Display Manager gdmchooser Format String Vulnerability

---

## SUMMARY

The gdmchooser program provides XDMCP (X Display Manager Control Protocol) functionality to the GNOME Display Manager. This protocol allows a user to interact remote systems via the local X11 display. Local exploitation of a format string vulnerability in GNOME Foundation's GNOME Display Manager host chooser window (gdmchooser) could allow an unauthenticated attacker to execute arbitrary code on the affected system.

## DETAILS

Vulnerable Systems:

- \* gdm version 2.14.1-1

Immune Systems:

- \* gdm version 2.14.11
- \* gdm version 2.16.4
- \* gdm version 2.17.4

The vulnerability specifically exists in the handling of values entered when choosing a remote host to connect to from the current system. The

## [UNIX] GNOME Foundation Display Manager gdmchooser Format String Vulnerability

following snippet from gdmchooser.c shows the vulnerable code:

```
1395 msg = g_strdup_printf (_("Cannot find the host \"%s\". "  
1396 "Perhaps you have mistyped it."),  
1397 name);  
1398  
1399 dialog = ve_hig_dialog_new  
1400 (GTK_WINDOW (chooser) /* parent */,  
1401 GTK_DIALOG_MODAL /* flags */,  
1402 GTK_MESSAGE_ERROR,  
1403 GTK_BUTTONS_OK,  
1404 _("Cannot find host"),  
1405 msg);  
1406  
1407 g_free (msg);  
1408
```

The error dialog uses the temporary value 'msg', constructed from 'name' when the host is not found. By supplying a sequence of formatting operations which modify memory values, an unauthenticated attacker can execute code with the permissions under the gdm account.

Analysis:

Successful local exploitation of this vulnerability would allow an unauthenticated attacker to execute arbitrary code with the privileges of the gdm service.

In order to exploit this vulnerability, the attacker would need to have access to the system running gdmchooser. Connecting remotely to this service will not work as the functionality is designed to connect to a remote server already, and proxying is not allowed.

The attacker selects the option to run the gdmchooser, and then types the format string into the dialog box. They can send a string which displays the contents of the stack, and use there construct a format string which will write controlled values to arbitrary memory locations, which allows execution of code with the privileges of the gdmchooser, typically the user 'gdm'. Although this user does not have a high privilege level, once this account has been gained, it would be relatively simple to insert a logger into gdm processes to capture other users passwords.

The gdmchooser is not accessible from the default login screens in any of the tested Red Hat systems, however the preferences utility does contain some preset screens which do contain it.

Workaround:

If XDMCP functionality is not required, setting the permissions on the gdmchooser to not allow execution will prevent any attempts at exploitation.

Vendor response:

[UNIX] GNOME Foundation Display Manager gdmchooser Format String Vulnerability

The GNOME maintainers have addressed this problem by releasing versions 2.14.11, 2.16.4, and 2.17.4 of the GNOME Display Manager.

Disclosure Timeline:

- 12/04/2006 – Initial vendor notification
- 12/05/2006 – Initial vendor response
- 12/14/2006 – Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by  
<<mailto:idlabs-advisories@xxxxxxxxxxxxx>> iDefense Labs Security Advisories.

The original article can be found at:  
<<http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=453>>  
<http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=453>

=====

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

=====

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.