

# [UNIX] Rrdbrowse Arbitrary File Disclosure Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-03/msg00019.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxx)>
  - *Date:* 5 Mar 2007 20:02:10 +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>

-----

Rrdbrowse Arbitrary File Disclosure Vulnerability

---

## SUMMARY

<<http://www.rrdbrowse.org>> RRDBrowse is "a poller daemon, templater and webinterface for RRDTOol. It has a threaded daemon which periodically runs from cron. It works with small .nfo files which hold router information and optionally connection details, colors, min max, bandwidth settings, etc, etc. RRDBrowse uses a small caching mechanism to store interface names. It's much MRTG like in it's current state". Due to improper input validation in rrdbrowse a remote attacker can cause the program to include arbitrary files and display their content.

## DETAILS

Vulnerable Systems:

- \* rrdbrowse version 1.6 and prior

Immune Systems:

- \* rrdbrowse version 1.7

Due to improper input validation, the CGI application "rrdbrowse" is vulnerable to an arbitrary file disclosure vulnerability. It allows an

## [UNIX] Rrdbrowse Arbitrary File Disclosure Vulnerability

unauthenticated remote attacker to read any file on the remote system if the user the webserver is running as has permissions to do so. Thus an attacker is able to gain access potentially sensitive information.

### Exploit:

The vulnerability is trivial to exploit and only requires specifying an URL with a relative file path on the remote system such as  
[http://\\$target/cgi-bin/rb.cgi?mode=page&file=../../../../../../../../etc/passwd](http://$target/cgi-bin/rb.cgi?mode=page&file=../../../../../../../../etc/passwd)

As the input to the "file" parameter is not validated in any way accessing this URL will expose the contents of /etc/passwd to a remote attacker (interestingly except the first line).

### Workaround:

To address this problem, the author of rrdbrowse (Tommy van Leeuwen) has released an updated CVS version (1.7) of the software which is available at <<http://www.rrdbrowse.org>> <http://www.rrdbrowse.org>. Hence all users of rrdbrowse are asked to test and install this version as soon as possible.

### Disclosure Timeline:

- 06. February 2007 – Notified vendor
- 14. February 2007 – Patch/new version released
- 04. March 2007 – Public disclosure

## ADDITIONAL INFORMATION

The information has been provided by <<mailto:sebastian@xxxxxxxxxxxxxxxx>>  
Sebastian Wolfgarten.

=====

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.