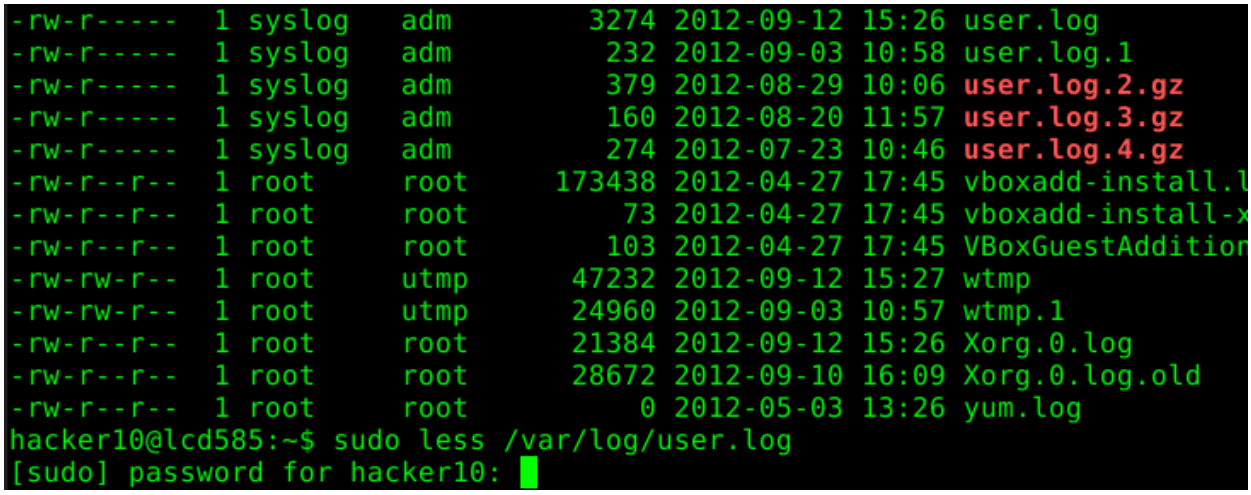
Dangerous Sudoers Entries – PART 2: Insecure Functionality

OCTOBER 8, 2012 / STEFAN HORLACHER / 0 COMMENTS

The following article describes common security issues regarding misconfigured sudoers' files. The article focuses on a single entry which contains several security issues:

```
hacker10 ALL= (root) /bin/less /var/log/*
```



The article is split into the following five chapters:

- PART 1: Command Execution
- **PART 2: Insecure Functionality**
- PART 3: Permissions
- PART 4: Wildcards
- PART 5: Recapitulation

In this article we are going to focus on insecure functionality “less” offers. The example with “less” is just to illustrate that the functionality of each application we use with “sudo” has to be checked carefully to ensure that a malicious user won’t be able to abuse it.

“less” offers a command to read other files on the system. Again, the current permissions of “less” are used to read these files.

Excerpt from the man page:

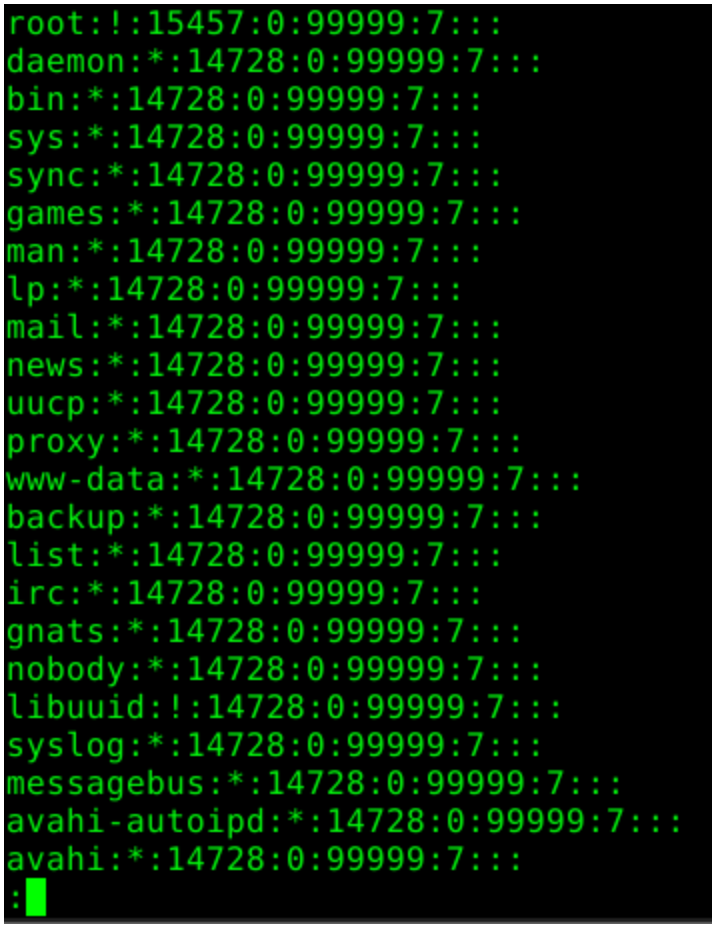
```
:e [filename]

Examine a new file. If the filename is missing, the "current"
file
(see the :n and :p commands below) from the list of files in
the
command line is re-examined. A percent sign (%) in the
filename
```

```
is replaced by the name of the current file. A pound sign (#)
is
replaced by the name of the previously examined file. However,
two
consecutive percent signs are simply replaced with a single
percent
sign. This allows you to enter a filename that contains a
percent
sign in the name. Similarly, two consecutive pound signs are
replaced with a single pound sign. The filename is inserted
into
the command line list of files so that it can be seen by
subsequent
:n and :p commands. If the filename consists of several files,
they
are all inserted into the list of files and the first one is
examined. If the filename contains one or more spaces, the
entire
filename should be enclosed in double quotes (also see the -"
option).
```

In the following example the /etc/shadow file has been read.

```
in the ALSA driver 'snd_intel8x0'. Please report this issue to the ALSA develope
rs.
Examine: /etc/shadow
```



Solution

The environment variable “LESSSECURE” can be set to “1” to disable dangerous features of “less”.

Excerpt from the man pages:

```
When the environment variable LESSSECURE is set to 1, less
runs in a "secure" mode. This means these features are
disabled:
!      the shell command
|      the pipe command
:e     the examine command.
v      the editing command
s -o  log files
-k     use of lesskey files
-t     use of tags files
metacharacters in filenames, such as *
```

```
filename completion (TAB, ^L)
Less can also be compiled to be permanently in "secure" mode.
```

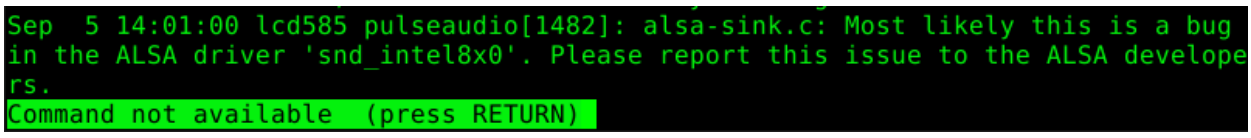
There are now two steps we have to take to ensure that this works as expected. First, the current user must have the “LESSSECURE” environment variable set as read-only. Otherwise the user would be able to change its value. This can be achieved by adding the following line to a file in the path “/etc/profile.d/”. We use a new file called “/etc/profile.d/lesssecure.sh” and add the following content:

```
LESSSECURE=1
readonly LESSSECURE
export LESSSECURE
```

The second step is to tell “sudo” to keep the “LESSSECURE” variable from the user. This is achieved by adding the *env_keep* option in the sudoer’s file:

```
Defaults        env_reset, env_keep=LESSSECURE
```

The following message appears now if someone tries to use one of the insecure commands.



Hardening, Linux

HARDENING LESS LINUX SUDO SUDOERS

PREVIOUS POST
Dangerous Sudoers Entries – PART 1: Command Execution

NEXT POST
Dangerous Sudoers Entries – PART 3: Permissions

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment *

Name *

Email *

Post Comment

Legal

RSS Feed

© 2026 COMPASS SECURITY BLOG

UP ↑