

[UNIX] Sudo Race Condition Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-06/0098.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 06/23/05

To: list@securiteam.com

Date: 23 Jun 2005 13:17:00 +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>

Sudo Race Condition Vulnerability

SUMMARY

" <<http://www.sudo.ws/>> Sudo (superuser do) allows a system administrator to give certain users (or groups of users) the ability to run some (or all) commands as root while logging all commands and arguments."

A race condition with the Sudo command pathname handling allows a local user with Sudo privileges to run arbitrary commands.

DETAILS

Vulnerable Systems:

- * Sudo version 1.3.1 up to version 1.6.8p8

Immune Systems:

- * Sudo version 1.6.8p9

When a user runs a command via Sudo, the inode and device numbers of the command are compared to those of commands with the same base-name found in the sudoers file. When a match is found, the path to the matching command listed in the sudoers file is stored in the variable `safe_cmnd`, which is later used to execute the command.

Securiteam: [UNIX] Sudo Race Condition Vulnerability

Because the actual path executed comes from the sudoers file and not directly from the user, Sudo should be safe from race conditions involving symbolic links. However, if a sudoers entry containing the pseudo-command ALL follows the user's sudoers entry the contents of safe_cmnd will be overwritten with the path the user specified on the command line, making Sudo vulnerable to the aforementioned race condition.

Example:

```
/etc/sudoers
root server=ALL
someuser server=/bin/echo
```

Whereas this one would be:

```
someuser server=/bin/echo
root server=ALL
```

Exploitation of the bug requires that the user be allowed to run one or more commands via Sudo and be able to create symbolic links in the filesystem. Furthermore, a sudoers entry giving another user access to the ALL pseudo-command must follow the user's sudoers entry for the race to exist.

Workaround:

The administrator can order the sudoers file such that all entries granting Sudo ALL privileges precede all other entries.

ADDITIONAL INFORMATION

The information has been provided by <mailto:Todd.Miller@courtesan.com>
Todd C. Miller.

The vendor advisory can be found at:
<http://www.sudo.ws/sudo/alerts/path_race.html>
http://www.sudo.ws/sudo/alerts/path_race.html

=====

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.