

[UNIX] Security Vulnerability Found in Sawmill (Incorrect Permissions)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-02/0083.html>

From: support@securiteam.com

Date: 02/14/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 14 Feb 2002 19:18:09 +0100 (CET)

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.

Security Vulnerability Found in Sawmill (Incorrect Permissions)

SUMMARY

<<http://www.sawmill.net/>> Sawmill is a powerful, hierarchical log analysis tool that runs on every major platform.

A sensitive file is created with world-readable rights, and this exposes the password file to all local users.

DETAILS

Vulnerable systems:

Sawmill version 6.2.14 and prior

Immune systems:

Sawmill version 6.2.15

When the Sawmill executable is launched and the user enters an initial password, the password is saved in file AdminPassword. This file is created mode 0666 (world read/writeable permissions).

This happens regardless of the password_file_permissions setting in file DefaultConfig, which is by default set to mode 0600.

Securiteam: [UNIX] Security Vulnerability Found in Sawmill (Incorrect Permissions)

The default path to file AdminPassword is accessible to users. The LogAnalysisInfo directory is created mode 0755.

The contents of the AdminPassword file are MD5'ed. It is trivial to overwrite this value with a password of our choosing:

```
"rm AdminPassword; echo mypasswd | perl -p -e 'chomp' | md5sum | \  
| sed 's/ -//' | perl -p -e 'chomp' > AdminPassword"
```

Solution:

```
Upgrade to version 6.2.15 or run:  
# chmod 600 AdminPassword
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:darky0da@hushmail.com>
darky0da.

=====

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: "[NT] InstantServers MiniPortal Multiple Vulnerabilities"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)