

[UNIX] log4sh Insecure Temporary Files Creation Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-07/0012.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/06/05

To: list@securiteam.com

Date: 6 Jul 2005 14:27:45 +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>

log4sh Insecure Temporary Files Creation Vulnerability

SUMMARY

" <<http://forestent.com/products/log4sh/>> Log4sh runs along the same lines as the other excellent logging services from the Apache Software Foundation. It adds to that list the ability to integrate powerful logging capabilities into a shell script."

log4sh creates temporally files in an insecure way allowing local attackers to gain elevated privileges.

DETAILS

Vulnerable Systems:

* log4sh versions 1.2.5 and prior

The vulnerability is caused due to temporary files being created insecurely. This can be exploited via a symlink attack, and in turn create and/or overwrite arbitrary files with the privileges of the user running the affected script.

Vulnerable code:

Securiteam: [UNIX] log4sh Insecure Temporary Files Creation Vulnerability

```
356 log4sh_readProperties()
357 {
358   _file=$1
359
360   _tmpFile="/tmp/log4sh.$$"
361   grep "^log4sh\." $_file >$_tmpFile
```

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1915>>
CAN-2005-1915

Disclosure Timeline:

26.05.05 – Discovered
09.06.05 – Vendor notified
27.06.05 – No response, Vendor Sec report (vendor-sec@lst.de)
04.07.05 – Disclosure

ADDITIONAL INFORMATION

The original article can be found at:

<<http://www.zataz.net/adviso/log4sh-06092005.txt>>

<http://www.zataz.net/adviso/log4sh-06092005.txt>

Gentoo Bugs Reports: <http://bugs.gentoo.org/show_bug.cgi?id=94069>

http://bugs.gentoo.org/show_bug.cgi?id=94069

=====

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.