

[UNIX] shtool Insecure Temporary File Creation

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0073.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/16/05

To: list@securiteam.com

Date: 16 Aug 2005 18:06:11 +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>

shtool Insecure Temporary File Creation

SUMMARY

<<http://www.gnu.org/software/shtool/>> GNU shtool is "a compilation of small but very stable and portable shell scripts into a single shell tool".

Shtool contains a security flaw that allows a malicious local user to create or overwrite content of arbitrary files with the rights of the user using shtool.

DETAILS

Vulnerable Systems:

* Shtool versions 2.0.1 and prior

The vulnerability is a race condition vulnerability.

A lot off products use shtool, for example:

oacan-mysql, SellaNMS, ipcmp, OOPSE, OpenLDAP, PHP, OpenPKG, ..

Vulnerable code :

```
572 # establish a temporary file on request
573 if [ ".$gen_tmpfile" = .yes ]; then
```

Securiteam: [UNIX] shtool Insecure Temporary File Creation

```
574 if [ ".$TMPDIR" != . ]; then
575 tmpdir="$TMPDIR"
576 elif [ ".$TEMPDIR" != . ]; then
577 tmpdir="$TEMPDIR"
578 else
579 tmpdir="/tmp"
580 fi
581 tmpfile="$tmpdir/.shtool.$$"
582 rm -f $tmpfile >/dev/null 2>&1
583 touch $tmpfile
584 chmod 600 $tmpfile
585 fi
..
597 # cleanup procedure
598 shtool_exit () {
599 rc="$1"
600 if [ ".$gen_tmpfile" = .yes ]; then
601 rm -f $tmpfile >/dev/null 2>&1 || true
602 fi
603 exit $rc
604 }
```

Workaround:

Use mktemp, umask and chmod to create secure temporary file.

Bug report:

<http://bugs.gentoo.org/show_bug.cgi?id=93782>
http://bugs.gentoo.org/show_bug.cgi?id=93782

Disclosure Timeline:

25.05.05 – Discovered
25.05.05 – Vendor notified
25.05.05 – Disclosure

ADDITIONAL INFORMATION

The information has been provided by <mailto:eromang@zataz.net> Eric Romang.

=====

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.

Securiteam: [UNIX] shtool Insecure Temporary File Creation

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.