

RE: Generic way to exploit an insecure /tmp file creation – Red Hat 7,8,9 (Re: Red Hat 9: free tickets)

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/vuln-dev/2003-07/0016.html>

From: Paul Vet (paul.vet_at_baldhead.com)

Date: 07/11/03

To: <vuln-dev@securityfocus.com>, <bugtraq@securityfocus.com>

Date: Fri, 11 Jul 2003 15:13:24 -0400

> *I believe that PERL actually has a pragma that you can set that
> should cause it to complain about cases like this. (sorry --
> don't have my book here with me).*

Indeed, any security conscious program should validate any external data before doing anything with it. Perl has Taint mode to enforce this (well, at least to pass the buck to the programmer). From perlsec (<http://www.perldoc.com/perl5.8.0/pod/perlsec.html>):

You may not use data derived from outside your program to affect something else outside your program—at least, not by accident. All command line arguments, environment variables, locale information (see perllocale), results of certain system calls (readdir(), readlink(), the variable of shmread(), the messages returned by msgrcv(), the password, gcos and shell fields returned by the getpwxxx() calls), and all file input are marked as "tainted". Tainted data may not be used directly or indirectly in any command that invokes a sub-shell, nor in any command that modifies files, directories, or processes, with the following exceptions...

****snip****

> *I actually **would** describe the bug below as a logwatch bug.*
> *If you have a uid=0 program calling shell scripts from*
> *data like filenames, those filenames should be sanitized.*
> *It would be easy enough to scan the filename for unexpected*
> *characters and refuse to use them on that basis.*
>
> *something as simple as:*
>
> *if (\$command =~ /^[^w]{*
> *carp "Unexpected filename: [[\$LogFile]]. Not used\n"*
> *}else{*
> *`/bin/cat \$Command`;*
> *};*

RE: Generic way to exploit an insecure /tmp file creation – Red Hat 7,8,9 (Re: Red Hat 9: free tickets)

>

Definitely a logwatch bug. Modifying your code to work with taint mode,

```
if ($Command =~ /(w*)/) { #match only on 'word' characters
    $Command = $1; #save the untainted match
    ... #do whatever
} else {
    carp "Unexpected filename: [[$Command]]. Not used\n"
}
```

Hopefully someone notified the Logwatch people...

Paul Vet.

> *Spybreak wrote:*

> > *On Wed, 2 Jul 2003, Michal Zalewski wrote:*

> > > *As far as I know, there was no neat and generic way to exploit an*

> > > *insecure /tmp file creation alone – well, until now.*

> > > >

> > > > *What Logwatch basically does, is feeding the logfiles through filter*

> > > > *scripts and emailing the results to a designated user (root by default).*

> > > > *But the whole issue is in the way how it is done.*

> > > > >

> > > > > *if (\$FileText) {*

> > > > > *my \$Command = \$FileText . \$FilterText . ">" . \$TempDir . \$LogFile;*

> > > > > *if (\$Config{'debug'}>4) {*

> > > > > *print "\nPreprocessing LogFile: " . \$LogFile . "\n" .*

> > > > > *\$Command . "\n";*

> > > > > *}*

> > > > > *`/bin/cat \$Command`;*

> > > > > *}*

> > > > > >

> > > > > > *It means if we create a file with a name of the form \`command\`*

> > > > > > *in one of these directories, the command gets executed with root privs,*

> > > > > > *when Logwatch is run by the cron daemon. And it doesn't matter,*

> > > > > > *what the*

> > > > > > *content of the created file is. What does matter is the filename.*

> > > > > > >

> > > > > > > *While this is not a Logwatch bug by itself, because the filter-script*

> > > > > > > *directories are writable only by root, it is a very helpful _flaw_*

> > > > > > > *once we have an above mentioned insecure file creation issue in*

> > > > > > > *some privileged code, and provides an easy root access.*

> > > > > > > >

> > > > > > > > >

> > > > > > > > > >

> > > > > > > > > > *Stephen Samuel +1(604)876-0426 samuel@bcgreen.com*

> > > > > > > > > > *<http://www.bcgreen.com/~samuel/>*

> > > > > > > > > > *Powerful committed communication. Transformation touching*

> > > > > > > > > > *the jewel within each person and bring it to life.*

> > > > > > > > > > >

SecurityFocus Vuln-Dev: RE: Generic way to exploit an insecure /tmp file creation – Red Hat 7,8,9 (Re: Red Hat 9: free ticket)

>

RE: Generic way to exploit an insecure /tmp file creation – Red Hat 7,8,9 (Re: Red Hat 9: free ticket)