

[UNIX] SGI IRIX inpview Design Error Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0065.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/16/05

To: list@securiteam.com

Date: 16 Jan 2005 10:53:15 +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>

SGI IRIX inpview Design Error Vulnerability

SUMMARY

The inpview program is "a setuid root application that is included in the InPerson networked multimedia conferencing tool. InPerson networked multimedia conferencing tool is included in SGI IRIX".

Local exploitation of a design error vulnerability in the inpview command included in multiple versions of Silicon Graphics Inc.'s IRIX could allow for arbitrary code execution as the root user.

DETAILS

Vulnerable Systems:

* SGI IRIX version 6.5.9 (feature) and version 6.5.22 (maintenance)

The vulnerability specifically exists due to the fact that inpview trusts the user environment and does not drop privileges. When the environment variable `SUN_TTSESSION_CMD` is something such as `"cp /bin/jsh /tmp/jsh;chmod 6755 /tmp/jsh;killall -9 inpview,"` the chain of commands will be executed with root permissions, thus allowing a regular user to drop a setuid and setgid shell to /tmp.

Analysis:

Securiteam: [UNIX] SGI IRIX inpview Design Error Vulnerability

All that is required to exploit this vulnerability is a local account and an open X display, which could be the attacker's home machine or another compromised system. Exploitation does not require any knowledge of application internals, making privilege escalation trivial, even for unskilled attackers.

Workaround:

Only allow trusted users local access to security critical systems.

Alternately, remove the setuid bit from inpview:

```
chmod u-s /usr/lib/InPerson/inpview
```

Vendor response:

Support for the InPerson product did not extend beyond 02/2002 as noted in the following publication:

<<http://techpubs.sgi.com/library/manuals/4000/007-4526-001/pdf/007-4526-001.pdf>>
<http://techpubs.sgi.com/library/manuals/4000/007-4526-001/pdf/007-4526-001.pdf>

As a result, no patch will be issued for this vulnerability.

Disclosure Timeline:

01/06/2005 – Initial vendor notification

01/07/2005 – Initial vendor response

01/13/2005 – Public disclosure

ADDITIONAL INFORMATION

The information has been provided by

<<mailto:idlabs-advisories@idefense.com>> iDEFENSE.

The original article can be found at:

<<http://www.idefense.com/application/poi/display?id=182&type=vulnerabilities>>
<http://www.idefense.com/application/poi/display?id=182&type=vulnerabilities>

=====

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.