

[UNIX] OpenSLP Initscript Symlink Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-08/0075.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/24/03

To: list@securiteam.com

Date: 24 Aug 2003 19:05:43 +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>

OpenSLP Initscript Symlink Vulnerability

SUMMARY

<<http://www.openslp.org>> OpenSLP is "an implementation of the 'Service Location Protocol V2', an IETF standards track protocol that provides a framework to allow networking applications to discover the existence, location, and configuration of networked services in enterprise networks".

There is symbolic link vulnerability in one of the initscripts provided with OpenSLP. The `slpd.all_init` file uses `/tmp/route.check` as a temporarily file in an unsafe manner.

DETAILS

Vulnerable systems:

- * OpenSLP version 1.0.11

Since the `slpd.all_init` script is usually called by the root user (to start the service), an attacker could exploit this vulnerability to at least "reset" the content of any file in the system as soon as the "start" action is called. As a standard symlink vulnerability, all the attacker needs is to create a `/tmp/route.check` symlink pointing to a system file.

Fortunately, the aforementioned initscript is not used by many vendors

Securiteam: [UNIX] OpenSLP Initscript Symlink Vulnerability

(only Conectiva, accordingly to a vendor-sec discussion). Debian distributes OpenSLP but uses another script.

Vulnerable code:

From the slpd.all_init file:

```
...
TMP_FILE=/tmp/route.check
...
ping ... > $TMP_FILE
...
rm -f $TMP_FILE
...
```

Vendor status:

The OpenSLP maintainers and the people from vendor-sec were contacted on 2003-Aug-07 and agreed on this disclosure date.

ADDITIONAL INFORMATION

The information has been provided by <mailto:ademar@conectiva.com.br>
Ademar de Souza Reis Jr..

=====

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.