

# [UNIX] Sun Management Console Directory Traversal Vulnerability

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-05/0054.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 05/16/04

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 16 May 2004 18:07:22 +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>

-----

Sun Management Console Directory Traversal Vulnerability

---

## SUMMARY

The Sun Management Console (SMC) webserver that runs on port 898 on Solaris 9, contains a vulnerability allowing a remote attacker to utilize a directory traversal vulnerability to disclose whether a file exists or not, by looking into the 404 error resulting in that directory traversal vulnerability.

## DETAILS

The quick summary is that it returns different 404 errors depending on where in the code the web server decides to call `sendError()`. If the file requested by the user does not exist, then the following is called:

```
httpservletresponse.sendError(404, "File Not Found<br>" + file);
```

Which results in an error page similar to:

```
Error: 404  
File Not Found  
/stuff/blah
```

If the file requested by the user does exist, but cannot be accessed for a

## Securiteam: [UNIX] Sun Management Console Directory Traversal Vulnerability

particular reason (i.e. file.getAbsolutePath() and file.getCanonicalPath() don't match), then the following is called:

```
httpServletResponse.sendError(404);
```

Which results in an error page similar to:

Error: 404

No detailed message

Unfortunately, no checks are done to see that the requested URL doesn't traverse out of the web root (typically /usr/sadm/lib/smc/htdocs) prior to calls to serveDir() or serveFile(), so these two functions happily access any path specified with root privileges.

Although it doesn't look to be possible to access files outside the web root, the differing error messages can tell remote users if a file or directory anywhere on the target system exists, which is a good bit of information disclosure especially since this service runs as root. As an example of interesting things to request, try the following:

<http://yourhost:898/../../../../tmp/.X11-unix>

<http://yourhost:898/../../../../rhosts>

<http://yourhost:898/../../../../ssh>

<http://yourhost:898/../../../../var/yp>

Which will answer interesting questions like "does my target run X-windows?", "do the administrators of this machine use r-services to administer the machine?", "do the administrators of this machine login as root using ssh?" and "does my target use NIS/yp?" The possibilities of this attack are only limited by an attacker's imagination.

### ADDITIONAL INFORMATION

The information has been provided by <mailto:warchild@spoofed.org> Jon Hart.

=====

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.