

[RISE-2008001] Sun Solstice AdminSuite sadmind adm_build_path() Buffer Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2008-10/msg00103.html>

- *From:* RISE Security <advisories@xxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 14 Oct 2008 11:43:29 -0300
-

RISE-2008001

Sun Solstice AdminSuite sadmind adm_build_path() Buffer Overflow Vulnerability

<http://risesecurity.org/advisories/RISE-2008001.txt>

Published: October 14, 2008

Updated: October 14, 2008

INTRODUCTION

There exists a vulnerability within a function of the Sun Solstice AdminSuite sadmind, which when properly exploited can lead to remote compromise of the vulnerable system.

This vulnerability was confirmed by us in the following versions of the Sun operating system, other versions may be also affected.

Sun Solaris 9 SPARC

Sun Solaris 9 x86

Sun Solaris 8 SPARC

Sun Solaris 8 x86

DETAILS

Solstice AdminSuite is a collection of graphical user interface tools and commands used to perform administrative tasks such as managing users, groups, hosts, system files, printers, disks, file systems, terminals, and modems.

The distributed system administration daemon (sadmind) is the daemon used by Solstice AdminSuite applications to perform distributed system administration operations.

The sadmind daemon is started automatically by the inetd daemon whenever a request to invoke an operation is received. The sadmind daemon process continues to run for 15 minutes after the last request is completed, unless a different idle-time is specified with the `-i` command line option. The sadmind daemon may be started independently from the command line, for example, at system boot time. In this case, the `-i` option has no effect; sadmind continues to run, even if there are no active requests.

[RISE-2008001] Sun Solstice AdminSuite sadmind adm_build_path() Buffer Overflow Vulnerability

The vulnerable function `adm_build_path()` does not validate user supplied data when appending it to a stack-based buffer using `strcat()`, resulting in a stack-based buffer overflow. The exploitation of this vulnerability is trivial and results in remote compromise of the vulnerable system.

This is the debug information about this vulnerability (from Sun Solaris 9 x86).

```
Breakpoint 1, 0xd330e5b0 in adm_build_path ()
from /usr/snadm/lib/libadmapm.so.2
(gdb) until *adm_build_path+38
0xd330e5c6 in adm_build_path () from /usr/snadm/lib/libadmapm.so.2
(gdb) x/i $pc
0xd330e5c6 <adm_build_path+38>: call 0xd3304fa8 <strcat@plt>
(gdb) x/x $esp+4
0x80411e4: 0x080b7cd0
(gdb) x/x $esp
0x80411e0: 0x08041208
(gdb) x/s 0x080b7cd0
0x80b7cd0: 'A' <repeats 200 times>...
(gdb) x/s 0x08041208
0x8041208: "system.2.1/"
(gdb) where
#0 0xd330e5c6 in adm_build_path () from /usr/snadm/lib/libadmapm.so.2
#1 0xd330eaa7 in adm_find_method () from /usr/snadm/lib/libadmapm.so.2
#2 0xd335326b in verify_vers_1 () from /usr/snadm/lib/libadmagt.so.2
#3 0xd3352e88 in verify_validate () from /usr/snadm/lib/libadmagt.so.2
#4 0xd3352cf8 in amsl_verify () from /usr/snadm/lib/libadmagt.so.2
#5 0xd32c8a85 in __ofQNetmgtDispatcherPdispatchRequestP6Hsvc_reqP6J__svcxpvt
() from /usr/snadm/lib/libadmcom.so.2
#6 0xd32c8656 in __ofQNetmgtDispatcherOreceiveRequestP6Hsvc_reqP6J__svcxpvt ()
from /usr/snadm/lib/libadmcom.so.2
#7 0xd32c837c in _netmgt_receiveRequest () from /usr/snadm/lib/libadmcom.so.2
#8 0xd311d4a3 in _svc_prog_dispatch () from /usr/lib/libnsl.so.1
#9 0xd311d24e in svc_getreq_common () from /usr/lib/libnsl.so.1
#10 0xd311d130 in svc_getreq_poll () from /usr/lib/libnsl.so.1
#11 0xd3121550 in _svc_run () from /usr/lib/libnsl.so.1
#12 0xd3121293 in svc_run () from /usr/lib/libnsl.so.1
#13 0xd32cd165 in __ofQNetmgtDispatcherNstartupServerv ()
from /usr/snadm/lib/libadmcom.so.2
#14 0xd32cd13b in netmgt_start_agent () from /usr/snadm/lib/libadmcom.so.2
#15 0x0805168f in main ()
(gdb) stepi
0xd3304fa8 in strcat@plt () from /usr/snadm/lib/libadmapm.so.2
(gdb) step
Single stepping until exit from function strcat@plt,
which has no line number information.
0xd330e5cb in adm_build_path () from /usr/snadm/lib/libadmapm.so.2
(gdb) x/i $pc
0xd330e5cb <adm_build_path+43>: add $0x8,%esp
(gdb) where
#0 0xd330e5cb in adm_build_path () from /usr/snadm/lib/libadmapm.so.2
```

[RISE-2008001] Sun Solstice AdminSuite sadmind adm_build_path() Buffer Overflow Vulnerability

```
#1 0xd330eaa7 in adm_find_method () from /usr/snadm/lib/libadmapm.so.2
#2 0xaabbccdd in ?? ()
#3 0x08063000 in ?? ()
#4 0x08063128 in ?? ()
#5 0x080b7cd0 in ?? ()
#6 0x08041730 in ?? ()
#7 0x00000400 in ?? ()
#8 0x00000001 in ?? ()
#9 0xd336ac8c in ?? () from /usr/snadm/lib/libadmagt.so.2
#10 0x00000000 in ?? ()
(gdb) c
Continuing.
```

```
Breakpoint 1, 0xd330e5b0 in adm_build_path ()
from /usr/snadm/lib/libadmapm.so.2
(gdb) c
Continuing.
```

```
Program received signal SIGSEGV, Segmentation fault.
0xaabbccdd in ?? ()
(gdb)
```

A proof of concept code for this vulnerability can be downloaded from our website <http://risesecurity.org/>.

VENDOR

Sun Security Coordination Team was notified of this issue, proper corrections should be available soon. Meanwhile, we recommend disabling the distributed system administration daemon (sadmind).

CREDITS

This vulnerability was discovered by Adriano Lima <adriano@xxxxxxxxxxxxxxxxxx>.

DISCLAIMER

The authors reserve the right not to be responsible for the topicality, correctness, completeness or quality of the information provided in this document. Liability claims regarding damage caused by the use of any information provided, including any kind of information which is incomplete or incorrect, will therefore be rejected.

\$Id: RISE-2008001.txt 2 2008-10-14 14:40:53Z ramon \$