

[UNIX] Remote Root Exploitation of Default Solaris sadmind Setting

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-09/0054.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/16/03

To: list@securiteam.com

Date: 16 Sep 2003 17:40:32 +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>

Remote Root Exploitation of Default Solaris sadmind Setting

SUMMARY

Solstice AdminSuite is a set of tools packaged by Sun Microsystems Inc. in its Solaris operating system to help administrators manage systems remotely, centralize configuration information, and monitor software usage. The sadmind daemon is used by Solstice AdminSuite applications to perform these distributed system administration operations. The sadmind daemon is typically installed and enabled in a default Solaris installation.

An exploit has surfaced that allows remote attackers to execute arbitrary commands with super-user privileges against Solaris hosts running the default RPC authentication scheme in Solstice AdminSuite. This weakness is documented to some extent in Sun documentation,

<http://docs.sun.com/db/doc/816-0211/6m6nc676b?a=view>

<http://docs.sun.com/db/doc/816-0211/6m6nc676b?a=view>.

DETAILS

Vulnerable systems:

* SunOS 5.3 thru 5.9 (Solaris 2.x, 7, 8, 9)

Securiteam: [UNIX] Remote Root Exploitation of Default Solaris sadmind Setting

By sending a sequence of specially crafted Remote Procedure Call (RPC) requests to the sadmind daemon, an attacker can exploit this vulnerability to gain unauthorized root access to a vulnerable system. The sadmind daemon defaults to weak authentication (AUTH_SYS), making it possible for a remote attacker to send a sequence of specially crafted RPC packets to forge the client identity.

After the identity has been successfully forged, the attacker can invoke a feature within the daemon itself to execute a shell as root or, depending on the forged credential, any other valid user of the system. The daemon will execute the program of the attacker's choice; for example, spawning a reverse-network shell back to the attacker for input/output control. Under certain circumstances, a reverse-network shell could allow for the attacker to bypass firewalls and/or filters.

Analysis:

Because the nature of the weakness exists on the application level, successful exploitation does not require the use of machine-specific code, nor does it require any previous knowledge of the target's architecture. Therefore, any local or remote attacker could execute commands as root on a vulnerable system running the sadmind service. By default, sadmind is installed and started at system boot time on most default and fully patched installations of Solaris. While many other vendors rely on SUNRPC related routines from Sun, this design issue is confined to Sun's sadmind authentication implementation in Solaris.

The most inherent threat is if this exploit becomes packaged into a cross-platform worm were it to become publicly available.

Detection:

An exploit has been obtained and demonstrated in real-world conditions on systems running Solaris or Trusted Solaris operating systems running sadmind. Default installations of SunOS 5.3 thru 5.9 (Solaris 2.x, 7, 8, 9) on both the SPARC and _x86 platforms are susceptible. In addition, versions 7 and 8 of Trusted Solaris on both the SPARC and _x86 platforms are susceptible to exploitation. Exploitation occurs through an initial request through UDP or TCP port 111 (sunrpc).

Workarounds:

For Solaris hosts that do not require the Solstice AdminSuite related services, disable the sadmind service by commenting out the appropriate line in /etc/inetd.conf. Make sure to restart inetd after changing this file (e.g. pkill -HUP inetd).

For networks, ensure proper ingress filters are in place on the Internet router and firewall, especially on TCP and UDP port 111. For Solaris hosts that require the Solstice AdminSuite to be running, the authentication security settings of sadmind should be increased to STRONG (AUTH_DES) – this is not the default setting. This setting also requires the creation of NIS or NIS+ DES keys to have been created for each Solaris user and each host.

Securiteam: [UNIX] Remote Root Exploitation of Default Solaris sadmind Setting

In order to upgrade the authentication setting, the sadmind line in /etc/inetd.conf should be changed to look like the following:
100232/10 tli rpc/udp wait root /usr/sbin/sadmind sadmind -S 2

Sun also recommends using the Solaris Security Toolkit (JASS) to harden a Solaris system, <<http://www.sun.com/software/security/jass/>>
<http://www.sun.com/software/security/jass/> .

Vendor response:

Sun does not plan on releasing a patch for this issue. Because a working exploit now exists for this issue, Sun Microsystems Inc. is issuing Alert 56740 to ensure administrators have proactively applied the proper workarounds in the event this exploit or one like it becomes publicly available. Sun's alert is available at
<<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F56740>>
<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F56740>.

CVE Information:

The Mitre Corp.'s Common Vulnerabilities and Exposures (CVE) Project has assigned CAN-2003-0722 to this issue.

Disclosure Timeline:

26 AUG 2003 Exploit acquired by iDEFENSE
26 AUG 2003 Sun notified (security-alert@sun.com)
27 AUG 2003 Followup status request via phone
27 AUG 2003 Response from Derrick Scholl, Sun Security Coordination Team
02 SEP 2003 iDEFENSE clients notified
16 SEP 2003 Coordinated Public Disclosure

ADDITIONAL INFORMATION

The original advisory can be downloaded from:
<<http://www.odefense.com/advisory/09.16.03.txt>>
<http://www.odefense.com/advisory/09.16.03.txt>.

The information has been provided by <<mailto:listserv@odefense.com>>
iDEFENSE Labs, the vulnerability has been discovered by
<<mailto:markzielinski@mailblocks.com>> Mark Zielinski.

=====

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.

Securiteam: [UNIX] Remote Root Exploitation of Default Solaris sadmind Setting

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.