

[VulnWatch] sparc exploit for known solaris 8 kcms_configure overflow

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2002-07/0010.html>

From: Adam Slattery (helo@sunriselinux.com)

Date: 07/07/02

Date: Sun, 7 Jul 2002 09:49:51 -0700 (PDT)
From: Adam Slattery <helo@sunriselinux.com>
To: vulnwatch@vulnwatch.org

See <http://www.securityfocus.com/bid/2558> for the published details of the vulnerability. It's a classic local suid 0 buffer overflow in kcms_configure on solaris 8 systems. Sun issued a patch a LONG time ago. Sunsolve patch 111400-01.

This is an old vulnerability (04/2001), but I don't think there are any published exploits for sparc systems (I could only find i386). It works with the default addresses on both of the unpatched Solaris 8 systems I have access to. These were ironically very busy machines with a lot of users that stay reasonably well patched. I guess the admins didn't realize they needed the kcms patch, which doesn't say anything about a root compromise.

DESCRIPTION:

The overflow is in an sprintf() call that occurs when kcms_configure is called with -o -S blah [>1024 byte string]. The sprintf call is made from a library in the kcms suite, so this might be exploitable from other suid kcms tools (but kcms_configure is probably the most straight forward). It's a command line buffer overflow that's fairly easy to control as long as an attacker can keep the program from seg faulting before the second return (to the address in the overwritten saved i7 register). This is somewhat tricky because a lot of code gets executed between the overflow and the second return. I'm not sure if I've ever seen any published sparc exploits deal with this problem (it's not that hard though). I dealt with it by overwriting the saved i0-i7 and i0-i6[fp] registers with the address of a string of pointers in memory (found in a couple of minutes with gdb). If an attacker doesn't do this, various instructions (notably st, clr) end up trying to use invalid memory and causing a segmentation fault.

My exploit is well commented, and could probably even be used as a simple SPARC Solaris exploit tutorial.

VulnWatch: [VulnWatch] sparc exploit for known solaris 8 kcms_configure overflow

relevent links:

<http://www.securityfocus.com/bid/2558>

<http://sunsolve.Sun.COM/pub-cgi/retrieve.pl?doc=fpatches/111400>
kcms_sparc.c is attached.

– Adam Slattery

-
- TEXT/PLAIN attachment: [kcms_sparc.c](#)
-

- *Previous message:* [D4rkGr3y: "\[VulnWatch\] bug"](#)
- *Messages sorted by:* [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)