

[UNIX] Solaris Kernel Module Insertion Local Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-03/0074.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 03/25/04

To: list@securiteam.com

Date: 25 Mar 2004 16:56:54 +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>

Solaris Kernel Module Insertion Local Vulnerability

SUMMARY

A vulnerability in Solaris exists which permits a local non-privileged user to insert a user supplied kernel module. Once a kernel module is successfully integrated into the kernel, it effectively gives the malicious user root permissions on the system.

DETAILS

Vulnerable Systems:

* Solaris versions 2.6 through 10

The loading of a user-supplied module by a non-privileged user is possible due to a directory traversal bug in the `vfs_getvfssw()` function within the kernel. There are two system calls which can be used in order to trigger this vulnerability, namely `mount()` and `sysfs()`.

Patch Availability:

Sun has supplied a patch which mitigates the vulnerability. It can be found at

<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F57479&zone_32=category%3Asecurity>

Securiteam: [UNIX] Solaris Kernel Module Insertion Local Vulnerability

http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F57479&zone_32=category%3Asecurity.

ADDITIONAL INFORMATION

The information has been provided by <mailto:dave@immunitysec.com> Dave Aitel of Immunity Inc..

The original article can be found at:

<http://www.immunitysec.com/downloads/solaris_kernel_vfs.sxw.pdf>

http://www.immunitysec.com/downloads/solaris_kernel_vfs.sxw.pdf

=====

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.