

# [UNIX] Sun Microsystems Solaris FIFO FS Information Disclosure Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-10/msg00007.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 8 Oct 2007 20:06:43 +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 Microsystems Solaris FIFO FS Information Disclosure Vulnerability

---

## SUMMARY

<<http://www.sun.com/software/solaris/>> Solaris is a UNIX operating system developed by Sun Microsystems. Local exploitation of an integer signedness error in Sun Microsystems's Solaris could allow attackers to disclose sensitive information from memory.

## DETAILS

Vulnerable Systems:

\* Solaris version 10 on x86 and SPARC (It is suspected that earlier versions are also affected)

The FIFO FS (First In First Out File System) is a service provided by the kernel that is commonly used for IPC (InterProcess Communication). A FIFO is represented as a node in the file system, and is similar to the concept of named pipes in Windows.

The vulnerability exists in the kernel `ioctl()` handler for FIFOs. The `L_PEEK` `ioctl` is used to peek at a number of bytes contained in the FIFO without actually removing them from the queue. One of the arguments to

## [UNIX] Sun Microsystems Solaris FIFO FS Information Disclosure Vulnerability

this command, which represents the number of bytes to peek, is a signed integer value. Since this parameter is not properly validated, a negative value can cause large amounts of kernel memory contents to be disclosed.

Exploitation allows an attacker to view potentially sensitive information belonging to the kernel or other users. For example, the root password hash or encryption keys might be disclosed.

### Vendor Status:

Sun has addressed this vulnerability by releasing patches. For more information, consult Sun Alert 103061:

<<http://sunsolve.sun.com/search/document.do?assetkey=1-26-103061-1>>  
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-103061-1>

### Disclosure Timeline:

- \* 02/13/2007 – Initial vendor notification
- \* 02/15/2007 – Initial vendor response
- \* 10/02/2007 – Coordinated public disclosure

## ADDITIONAL INFORMATION

The information has been provided by iDefense.  
The original article can be found at:

<<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=603>>  
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=603>

=====

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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====  
=====

### 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.