

===[ ABSTRACT ]=====

A new vmsplice() system call was introduced in the 2.6.17 release of the Linux kernel. In the 2.6.23 kernel the system call functionality has been further extended resulting in two new critical vulnerabilities.

===[ AFFECTED SOFTWARE ]=====

Linux 2.6.23 - 2.6.24

For the exact kernel version please refer to an information provided by your vendor.

===[ DESCRIPTION ]=====

#### VULNERABILITY #1

Inappropriate dereference of user-supplied memory pointers in the code beginning at line 1378 in the vmsplice\_to\_user() kernel function (fs/splice.c):

```

---8<--- fs/splice.c:1378 ---8<---
    error = get_user(base, &iov->iov_base);
    /* ... */
    if (unlikely(!base)) {
        error = -EFAULT;
        break;
    }
    /* ... */
    sd.u.userptr = base;
    /* ... */
    size = __splice_from_pipe(pipe, &sd, pipe_to_user);
---8<--- fs/splice.c:1401 ---8<---

```

The code lacks validation of these pointers (i.e. with access\_ok()). The \_\_splice\_from\_pipe() assumes these are valid user-memory pointers and never makes any verification of them. The function dereferences the pointers with \_\_copy\_to\_user\_inatomic() function (in pipe\_to\_user()) in order to write data to user-process memory in this case leading to possibility of arbitrary data (read from pipe) to arbitrary kernel memory.

#### VULNERABILITY #2

The copy\_from\_user\_mmap\_sem() function copies data from user-process memory with the use of \_\_copy\_from\_user\_inatomic() without validating user-supplied pointer with access\_ok():

```

---8<--- fs/splice.c:1188 ---8<---
    partial = __copy_from_user_inatomic(dst, src, n);
---8<--- fs/splice.c:1188 ---8<---

```

This vulnerability leads to indirect reading of arbitrary kernel memory.

===[ IMPACT ]=====

Vulnerabilities may lead to local system compromise including execution of arbitrary machine code in the context of running kernel.

Vulnerability #1 has been successfully exploited on Linux 2.6.24.

Vulnerability #2 not tested.

===[ DISCLOSURE TIMELINE ]=====

1st Feb 2008      Vendor notification  
8th Feb 2008      Public disclosure

===[ AUTHOR ]=====

Wojciech Purczynski <cliph@research.coseinc.com>

Wojciech Purczynski is a Security Researcher at Vulnerability Research  
Labs, COSEINC PTE Ltd.  
<http://coseinc.com>

Wojciech Purczynski is also a member of iSEC Security Research  
<http://isec.pl/>

===[ LEGAL DISCLAIMER ]=====

Copyright (c) 2008 Wojciech Purczynski  
Copyright (c) 2008 COSEINC PTE Ltd.

All Rights Reserved.

PUBLISHING, DISTRIBUTING, PRINTING, COPYING, SCANNING, DUPLICATING IN  
ANY FORM, MODIFYING WITHOUT PRIOR WRITTEN PERMISSION IS STRICTLY  
PROHIBITED.

THE DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. THE  
CONTENT MAY CHANGE WITHOUT NOTICE. IN NO EVENT SHALL THE AUTHORS BE  
LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES, INJURIES,  
LOSSES OR UNLAWFUL OFFENCES.

USE AT YOUR OWN RISK.