

[UNIX] Linux Kernel Socket Buffer Memory Exhaustion DoS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00083.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 26 Dec 2005 18:57:17 +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>

Linux Kernel Socket Buffer Memory Exhaustion DoS

SUMMARY

<<http://www.kernel.org>> Linux is "a clone of the operating system Unix, written from scratch by Linus Torvalds with assistance from a loosely-knit team of hackers across the Net. It aims towards POSIX and Single UNIX Specification compliance".

Local exploitation of a memory exhaustion vulnerability in Linux Kernel versions 2.4 and 2.6 allow local attackers to cause a denial of service condition.

DETAILS

Vulnerable Systems:

- * Linux version 2.4.22
- * Linux version 2.6.12

The vulnerability specifically exists due to a lack of resource checking during the buffering of data for transfer over a pair of sockets. An attacker can create a situation that, depending on the amount of available system resources, can cause the kernel to panic due to memory resource

[UNIX] Linux Kernel Socket Buffer Memory Exhaustion DoS

exhaustion. The attack is conducted by opening up a number of connected file descriptors or socketpairs and creating the largest possible kernel buffer for the data transfer between the two sockets. By causing the process to enter a zombie state or closing the file descriptor while keeping a reference open, the data is kept in the kernel until the transfer can complete. If done repeatedly, system memory resources can be exhausted from the kernel.

Successful exploitation requires an attacker to have local access to an affected Linux system and can result in complete system denial of service. The system may not reboot after successful exploitation, requiring human interaction to be restored to a working state. Depending on available resources, systems with large amounts of physical memory may not be affected.

Vendor Status:

The maintainer acknowledges that this issue is a design limitation in the Linux kernel. The following advice has been offered for creating a patch. It should be noted that this patch has not been fully tested.

The patch requires three steps:

- 1) Add a "struct user *" reference to the "struct file" file structure.
- 2) Whenever creating a new "struct file" add the following code:

```
struct user *user = current->user;
```

```
if (atomic_read(&user->files) > MAX_FILES_FOR_THIS_USER)
return -EMFILE;
```

```
file->user = user;
if(user) {
atomic_inc(&user->count);
atomic_inc(&user->files);
}
```

- 3) Whenever a "struct file" is released apply the following code:

```
struct user *user = file->user;
```

```
if (user) {
atomic_dec(&user->files);
free_uid(user);
}
```

CVE Information:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3660>
CAN-2005-3660.

[UNIX] Linux Kernel Socket Buffer Memory Exhaustion DoS

Disclosure Timeline:

11/17/2005 Initial vendor notification – Linux vendors

11/19/2005 Initial vendor responses

12/22/2005 Public disclosure

ADDITIONAL INFORMATION

The information has been provided by

<<mailto:idlabs-advisories@xxxxxxxxxxxxxxxxxxxx>> iDEFENSE Labs.

The original article can be found at:

<<http://www.odefense.com/intelligence/vulnerabilities/display.php?id=362>>

<http://www.odefense.com/intelligence/vulnerabilities/display.php?id=362>

=====

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.

-
- Prev by Date: [*\[NT\] McAfee VirusScan Privileges Escalation*](#)
 - Next by Date: [*\[NEWS\] Electric Sheep Window-Id Local Stack Overflow*](#)
 - Previous by thread: [*\[NT\] McAfee VirusScan Privileges Escalation*](#)
 - Next by thread: [*\[NEWS\] Electric Sheep Window-Id Local Stack Overflow*](#)
 - Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)