

Linux Kernel SMP "/proc" Race Condition DoS

By *srlinuxx*

Created 31/05/2006 - 2:39pm

Submitted by srlinuxx on Wednesday 31st of May 2006 02:39:08 PM Filed under [Security](#) [1]

Tony Griffiths has reported a vulnerability in the Linux Kernel, which can be exploited malicious, local users to cause a DoS (Denial of Service).

The vulnerability is cause due to a memory corruption error in the "dentry_unused" list within the "prune_dcache()" function. This can be exploited to crash the kernel when running on SMP hardware by causing a race condition such that one or more tasks exit while another task is reading their /proc entries.

The vulnerability has been reported in versions 2.6.15 through 2.6.17. Other versions may also be affected.

[Full Story](#) [2].

[Security](#)

Source URL: <http://www.tuxmachines.org/node/7272>

Links:

[1] <http://www.tuxmachines.org/taxonomy/term/59>

[2] <http://secunia.com/advisories/20349/>