

More Linux kernel flaws: Multiple DoS and permission vulnerabilities

xiando

Updated kernels are available for Gentoo and other systems and users are encouraged to upgrade.

A remote attacker can mount your file-systems and change files group IDs if you are using a vulnerable 2.4 Linux kernel.

A new flaw is also found in the 2.6 series allowing unauthorized modification of entries in /proc, and this is a major security risk.

A VServer Linux specific /proc related issue is also found along with a local DoS vulnerability and a floating point information leak on IA64 platforms.

- [Linux Kernel: Multiple DoS and permission vulnerabilities](#)
(gentoo.org)
 - [Linux kernel has multiple flaws](#)
 - [CAN-2004-0447
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0447>
 - [CAN-2004-0496
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0496>
 - [CAN-2004-0497
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0497>
 - [CAN-2004-0565
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0565>
 - [VServer /proc Context Vulnerability](#)
-

> [Linux Reviews](#) > [News and headlines](#) > [2004 News archive](#) > [July](#) >
More Linux kernel flaws: Multiple DoS and permission vulnerabilities