

# Recent Linux vulnerabilities

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-01/0143.html>

---

**From:** Leonardo Eloy ([leonardo\\_at\\_morphus.com.br](mailto:leonardo_at_morphus.com.br))

**Date:** 01/18/05

Date: Tue, 18 Jan 2005 11:17:46 -0300

To: [pen-test@securityfocus.com](mailto:pen-test@securityfocus.com)

Hi list,

It's known that the Linux kernel has multiple vulnerabilities (I counted 22 just this month, listed below). In the audits I've been participating I turned my main test point to the Linux Kernel, when local user privilege has been achieved.

I was wondering, how many of you do really use these vulnerabilities when doing pen tests?

List of known kernel vulnerabilities in January/2005 (source: [securityfocus.com](http://securityfocus.com)):

2005-01-14: Linux Kernel SMBFS Multiple Remote Vulnerabilities

2005-01-14: Linux Kernel Multiple Local MOXA Serial Driver Buffer Overflow Vulnerabilities

2005-01-14: Linux Kernel ELF Binary Loading Denial Of Service Vulnerability

2005-01-14: Linux Kernel IGMP Multiple Vulnerabilities

2005-01-14: Linux Kernel USB io\_edgeport Driver Local Integer Overflow Vulnerability

2005-01-14: Linux Kernel SCM\_SEND Local Denial of Service Vulnerability

2005-01-14: Linux Kernel EXT3 File System Information Leakage Vulnerability

2005-01-14: Linux Kernel BINFORMAT\_ELF Loader Local Privilege Escalation Vulnerabilities

2005-01-14: Linux Kernel AF\_UNIX Arbitrary Kernel Memory Modification Vulnerability

2005-01-14: Linux Kernel USB Driver Uninitialized Structure Information Disclosure Vulnerability

2005-01-13: Linux Kernel User Triggerable BUG() Unspecified Local Denial of Service Vulnerability

2005-01-13: Linux Kernel Local Denial Of Service And Memory Disclosure Vulnerabilities

2005-01-13: Linux kernel Uselib() Local Privilege Escalation Vulnerability

2005-01-11: Linux Kernel Multiple Unspecified Vulnerabilities

## SecurityFocus Penetration: Recent Linux vulnerabilities

2005-01-11: Linux Kernel Local RLIMIT\_MEMLOCK Bypass Denial Of Service Vulnerability

2005-01-11: Linux Kernel SCSI IOCTL Integer Overflow Vulnerability

2005-01-11: Linux Kernel Random Poolsize SysCTL Handler Integer Overflow Vulnerability

2005-01-11: Linux Security Modules Process Capabilities Design Error Vulnerability

2005-01-05: Linux Kernel Local File Descriptor Passing Security Module Bypass Vulnerability

2005-01-05: Linux Kernel SYSENTER Thread Information Pointer Local Information Disclosure Vulnerability

2005-01-04: Linux Kernel Sock\_DGram\_SendMsg Local Denial Of Service Vulnerability

2005-01-04: Linux Kernel Multiple Local Vulnerabilities

Regards,

--

Leonardo Eloy, LPIC-1, FCSE

Security Analyst

Morphus Tecnologia

Fone/Fax: 85 3452.5733/5737

Móvel: 85 8802.6740

e-mail: [leonardo@morphus.com.br](mailto:leonardo@morphus.com.br)

site: <http://www.morphus.com.br>

The information contained in this message and in the attached files are restricted, and its confi