# CVE Detail – CVE-2002-0083

Off-by-one error in the channel code of OpenSSH 2.0 through 3.0.2 allows local users or remote malicious servers to gain privileges.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.80775

## CVSS Scoring

CVSS v3.1 Score: 9.8

Severity: CRITICAL

## Mapped CWE(s)

* CWE-193: Off-by-one Error

## Affected Products

* cpe:2.3:a:immunix:immunix:7.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:mandrakesoft:mandrake\_single\_network\_firewall:7.2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:openbsd:openssh:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:openpkg:openpkg:1.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:conectiva:linux:5.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:conectiva:linux:5.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:conectiva:linux:6.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:conectiva:linux:7.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:conectiva:linux:ecommerce:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:conectiva:linux:graficas:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:engardelinux:secure\_linux:1.0.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:mandrakesoft:mandrake\_linux:7.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:mandrakesoft:mandrake\_linux:7.2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:mandrakesoft:mandrake\_linux:8.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:mandrakesoft:mandrake\_linux:8.0:\*:ppc:\*:\*:\*:\*:\*
* cpe:2.3:o:mandrakesoft:mandrake\_linux:8.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:mandrakesoft:mandrake\_linux\_corporate\_server:1.0.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:linux:7.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:linux:7.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:linux:7.2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:suse\_linux:6.4:\*:i386:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:suse\_linux:6.4:\*:ppc:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:suse\_linux:6.4:alpha:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:suse\_linux:7.0:\*:i386:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:suse\_linux:7.0:\*:ppc:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:suse\_linux:7.0:\*:sparc:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:suse\_linux:7.0:alpha:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:suse\_linux:7.1:\*:spa:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:suse\_linux:7.1:\*:sparc:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:suse\_linux:7.1:\*:x86:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:suse\_linux:7.1:alpha:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:suse\_linux:7.2:\*:i386:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:suse\_linux:7.3:\*:i386:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:suse\_linux:7.3:\*:ppc:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:suse\_linux:7.3:\*:sparc:\*:\*:\*:\*:\*
* cpe:2.3:o:trustix:secure\_linux:1.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:trustix:secure\_linux:1.2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:trustix:secure\_linux:1.5:\*:\*:\*:\*:\*:\*:\*