



# CVE-2005-0750

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2005-0750
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2005-03-27 05:00:00 UTC
<b>Updated</b>	2017-10-11 01:30:00 UTC
<b>Description</b>	The bluez_sock_create function in the Bluetooth stack for Linux kernel 2.4.6 through 2.4.30-rc1 and 2.6 through 2.6.11.5 all

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Conectiva</a>	<a href="#">Linux</a>	10.0	All	All	All
Operating System	<a href="#">Conectiva</a>	<a href="#">Linux</a>	10.0	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.10	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.11	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.12	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.13	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.14	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.15	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.16	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.17	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.18	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.19	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.20	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.21	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.22	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.23	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.24	All	All	All

Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.25	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.26	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.27	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.28	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.29	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.6	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.7	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.8	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.9	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.0	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.1	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.10	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.11	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.2	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.3	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.4	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.5	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.6	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.7	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.8	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.9	2.6.20	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.10	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.11	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.12	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.13	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.14	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.15	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.16	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.17	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.18	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.19	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.20	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.21	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.22	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.4.23	All	All	All

Operating System	Linux	Linux Kernel	2.4.24	All	All	All
Operating System	Linux	Linux Kernel	2.4.25	All	All	All
Operating System	Linux	Linux Kernel	2.4.26	All	All	All
Operating System	Linux	Linux Kernel	2.4.27	All	All	All
Operating System	Linux	Linux Kernel	2.4.28	All	All	All
Operating System	Linux	Linux Kernel	2.4.29	All	All	All
Operating System	Linux	Linux Kernel	2.4.6	All	All	All
Operating System	Linux	Linux Kernel	2.4.7	All	All	All
Operating System	Linux	Linux Kernel	2.4.8	All	All	All
Operating System	Linux	Linux Kernel	2.4.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.0	All	All	All
Operating System	Linux	Linux Kernel	2.6.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.9	2.6.20	All	All
Operating System	Redhat	Enterprise Linux	4.0	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	workstation	All
Operating System	Redhat	Enterprise Linux	4.0	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	workstation	All
Operating System	Redhat	Enterprise Linux Desktop	4.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	4.0	All	All	All
Operating System	Redhat	Fedora Core	core_1.0	All	All	All
Operating System	Redhat	Fedora Core	core_2.0	All	All	All
Operating System	Redhat	Fedora Core	core_3.0	All	All	All
Operating System	Redhat	Fedora Core	core_1.0	All	All	All
Operating System	Redhat	Fedora Core	core_2.0	All	All	All

Operating System	<a href="#">Redhat</a>	<a href="#">Fedora Core</a>	core_3.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux</a>	7.3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux</a>	7.3	All	i386	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux</a>	7.3	All	i686	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux</a>	9.0	All	i386	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux</a>	7.3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux</a>	7.3	All	i386	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux</a>	7.3	All	i686	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux</a>	9.0	All	i386	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	1.0	All	desktop	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	9.3	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	1.0	All	desktop	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	9.3	All	All	All
Operating System	<a href="#">Ubuntu</a>	<a href="#">Ubuntu Linux</a>	4.1	All	ia64	All
Operating System	<a href="#">Ubuntu</a>	<a href="#">Ubuntu Linux</a>	4.1	All	ppc	All
Operating System	<a href="#">Ubuntu</a>	<a href="#">Ubuntu Linux</a>	4.1	All	ia64	All
Operating System	<a href="#">Ubuntu</a>	<a href="#">Ubuntu Linux</a>	4.1	All	ppc	All

## References

### Reference

152532 – Multiple kernel security problems: CAN-2005-0384, CAN-2005-0400, CAN-2005-0449, CAN-2005-0531(?), CAN-2005-0749, CAN-2

[rhnl.redhat.com | Red Hat Support](#)

[IBM X-Force Exchange](#)

[rhnl.redhat.com | Red Hat Support](#)

'local root security bug in linux >= 2.4.6 <= 2.4.30-rc1 and 2.6.x.y' - MARC

[Full-disclosure] local root security bug in linux >= 2.4.6 <= 2.4.30-rc1 and 2.6.x.y <= 2.6.11.5

[rhnl.redhat.com | Red Hat Support](#)

[rhnl.redhat.com | Red Hat Support](#)

[Linux Kernel Bluetooth Signed Buffer Index Vulnerability](#)

[Repository / Oval Repository](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**