



# CVE-2009-4484

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

## Summary

<b>CVE</b>	CVE-2009-4484
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2009-12-30 21:30:00 UTC
<b>Updated</b>	2023-02-14 21:13:00 UTC
<b>Description</b>	Multiple stack-based buffer overflows in the CertDecoder::GetName function in src/asn.cpp in TaoCrypt in yaSSL before 1.9

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.10	All	All	All
Operating System	Canonical	Ubuntu Linux	11.04	All	All	All
Operating System	Canonical	Ubuntu Linux	11.10	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	8.10	All	All	All
Operating System	Canonical	Ubuntu Linux	9.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.10	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.10	All	All	All
Operating System	Canonical	Ubuntu Linux	11.04	All	All	All
Operating System	Canonical	Ubuntu Linux	11.10	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	8.10	All	All	All
Operating System	Canonical	Ubuntu Linux	9.04	All	All	All

Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	9.10	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	5.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	6.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	5.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	6.0	All	All	All
Application	<a href="#">Mariadb</a>	<a href="#">Mariadb</a>	All	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Mysql</a>	All	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Mysql</a>	5.0.0	milestone1	All	All
Application	<a href="#">Oracle</a>	<a href="#">Mysql</a>	5.0.0	milestone2	All	All
Application	<a href="#">Oracle</a>	<a href="#">Mysql</a>	All	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Mysql</a>	5.0.0	milestone1	All	All
Application	<a href="#">Oracle</a>	<a href="#">Mysql</a>	5.0.0	milestone2	All	All
Application	<a href="#">Wolfssl</a>	<a href="#">Yassl</a>	All	All	All	All
Application	<a href="#">Wolfssl</a>	<a href="#">Yassl</a>	All	All	All	All

## References

Reference	Source
RETIRED: yaSSL SSL Certificate Handling Remote Buffer Overflow Vulnerability	BID
MySQL :: MySQL 5.1 Reference Manual :: C.1.1 Changes in MySQL 5.1.43 (Not yet released)	CONFIRM
Bug 555313 – CVE-2009-4484 mysql: yaSSL certificate parsing buffer overflow (vulndisco)	CONFIRM
Not Found	CONFIRM
Ubuntu update for mysql-dfsg-5 and mysql-dfsg-5.1 - Advisories - Community	SECUNIA
yaSSL Certificate Processing Buffer Overflow Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
IBM X-Force Exchange	XF
MySQL Unspecified Flaw Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRA
yaSSL   News Security Library	CONFIRM
MySQL :: MySQL 5.0 Reference Manual :: C.1.1 Changes in MySQL 5.0.90 (15 January 2010)	CONFIRM
NEOHAPSIS - Peace of Mind Through Integrity and Insight	MLIST
MySQL yaSSL Certificate Processing Buffer Overflow Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
USN-897-1: MySQL vulnerabilities   Ubuntu	UBUNTU
Debian -- Security Information -- DSA-1997-1 mysql-dfsg-5.0	DEBIAN
MySQL Bugs: Access denied	CONFIRM
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
SSL Certificate Processing Buffer Overflow Vulnerability	SECUNIA

yaSSL Certificate Processing Buffer Overflow Vulnerability - Secunia.com	SECUNIA
MySQL remote exploit demo	MISC
MySQL Lists: commits: bzd commit into mysql-5.0-bugteam branch (ramil:2838) Bug#50227	MLIST
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
VulnDisco Pack Professional 8.11 « Intevydis blog	MISC
404 Not Found	MISC
Metasploit Penetration Testing Framework - Module Browser	MISC
[dailydave] 20100126 New db bugs	MLIST
Debian update for mysql-dfsg-5.0 - Secunia.com	SECUNIA
MySQL with yaSSL SSL Certificate Handling Remote Stack Buffer Overflow Vulnerability	BID
61956	OSVDB
USN-1397-1: MySQL vulnerabilities   Ubuntu	UBUNTU
yaSSL   Release notes	CONFIRM
yaSSL Buffer Overflow in Certificate Processing Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRA
www.intevydis.com/blog	MISC
404 Not Found	MISC
Possible new MySQL 0day	MISC
Intevydis blog: MySQL yassl stack overflow	MISC
CVS Info for project yassl	CONFIRM
MySQL 5.0.51a Unspecified Remote Code Execution Vulnerability	BID
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

### Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2010-01-26	Tomas Hoger	Not vulnerable. This issue did not affect the versions of mysql as shipped with Red Hat Enterprise Linux 5.0-5.4.

### Legacy QID Mappings

<a href="#">900089</a> CBL-Mariner Linux Security Update for kernel 5.4.51
<a href="#">902862</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3462)
<a href="#">905912</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3462-1)

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](#)**