



CVE-2007-1888

Published on: 04/05/2007 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:36 PM UTC

CVE-2007-1888

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Php](#) from [Php](#) contain the following vulnerability:

Buffer overflow in the `sqlite_decode_binary` function in `src/encode.c` in SQLite 2, as used by PHP 4.x through 5.x and other applications, allows context-dependent attackers to execute arbitrary code via an empty value of the `in` parameter. NOTE: some PHP installations use a bundled version of sqlite without this vulnerability. The SQLite developer has argued that this issue could be due to a misuse of the `sqlite_decode_binary()` API.

CVE-2007-1888 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

Access
Complexity

Authentication

NETWORK

LOW

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

PARTIAL

PARTIAL

PARTIAL

CVE References

Description

Tags

Link

[VIM] vendor ack/clarification for CVE-2007-1888 (SQLite)

[www.attrition.org](#)
text/html

[VIM 20070422 vendor ack/clarification for CVE-2007-1888 \(SQLite\)](#)

USN-455-1: PHP vulnerabilities | Ubuntu

[www.ubuntu.com](#)
text/html

[UBUNTU USN-455-1](#)

Ubuntu update for php - Advisories - Secunia

[web.archive.org](#)
text/html

[SECUNIA 25057](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
text/html

[XF sqlite-sqlitedecodebinary-bo\(38518\)](#)

Not Found

[www.sqlite.org](#)
text/html

[MISC www.sqlite.org/cvstrac/rlog?f=sqlite/src/encode.c](#)

Inactive Link Not Archived

No Description Provided

osvdb.org

OSVDB 39177

Inactive Link Not Archived

MOPB-41-2007:PHP 5 sqlite_udf_decode_binary() Buffer Overflow Vulnerability

Patch

Vendor Advisory

web.archive.org

text/html

Inactive Link Not Archived

MISC www.php-security.org/MOPB/MOPB-41-2007.html

Advisories - Mandriva Linux

www.mandriva.com

text/html

MANDRIVA MDKSA-2007:091

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Php	Php	4.0	All	All	All
Application	Php	Php	4.0	beta1	All	All
Application	Php	Php	4.0	beta2	All	All
Application	Php	Php	4.0	beta3	All	All
Application	Php	Php	4.0	beta4	All	All
Application	Php	Php	4.0	beta_4_patch1	All	All
Application	Php	Php	4.0	rc1	All	All
Application	Php	Php	4.0	rc2	All	All
Application	Php	Php	4.0.0	All	All	All
Application	Php	Php	4.0.1	All	All	All
Application	Php	Php	4.0.1	patch1	All	All
Application	Php	Php	4.0.1	patch2	All	All
Application	Php	Php	4.0.2	All	All	All
Application	Php	Php	4.0.3	All	All	All
Application	Php	Php	4.0.3	patch1	All	All
Application	Php	Php	4.0.4	All	All	All
Application	Php	Php	4.0.4	patch1	All	All
Application	Php	Php	4.0.5	All	All	All
Application	Php	Php	4.0.6	All	All	All
Application	Php	Php	4.0.7	All	All	All

Application	Php	Php	4.0.7	rc1	All	All
Application	Php	Php	4.0.7	rc2	All	All
Application	Php	Php	4.0.7	rc3	All	All
Application	Php	Php	4.1.0	All	All	All
Application	Php	Php	4.1.1	All	All	All
Application	Php	Php	4.1.2	All	All	All
Application	Php	Php	4.2	All	dev	All
Application	Php	Php	4.2.0	All	All	All
Application	Php	Php	4.2.1	All	All	All
Application	Php	Php	4.2.2	All	All	All
Application	Php	Php	4.2.3	All	All	All
Application	Php	Php	4.3.0	All	All	All
Application	Php	Php	4.3.1	All	All	All
Application	Php	Php	4.3.10	All	All	All
Application	Php	Php	4.3.11	All	All	All
Application	Php	Php	4.3.2	All	All	All
Application	Php	Php	4.3.3	All	All	All
Application	Php	Php	4.3.4	All	All	All
Application	Php	Php	4.3.5	All	All	All
Application	Php	Php	4.3.6	All	All	All
Application	Php	Php	4.3.7	All	All	All
Application	Php	Php	4.3.8	All	All	All
Application	Php	Php	4.3.9	All	All	All
Application	Php	Php	4.4.0	All	All	All
Application	Php	Php	4.4.1	All	All	All
Application	Php	Php	4.4.2	All	All	All
Application	Php	Php	4.4.3	All	All	All
Application	Php	Php	4.4.4	All	All	All
Application	Php	Php	4.4.5	All	All	All
Application	Php	Php	4.4.6	All	All	All
Application	Php	Php	5.0	rc1	All	All
Application	Php	Php	5.0	rc2	All	All
Application	Php	Php	5.0	rc3	All	All
Application	Php	Php	5.0.0	All	All	All
Application	Php	Php	5.0.0	beta1	All	All

Application	Php	Php	5.0.0	beta2	All	All
Application	Php	Php	5.0.0	beta3	All	All
Application	Php	Php	5.0.0	beta4	All	All
Application	Php	Php	5.0.0	rc1	All	All
Application	Php	Php	5.0.0	rc2	All	All
Application	Php	Php	5.0.0	rc3	All	All
Application	Php	Php	5.0.1	All	All	All
Application	Php	Php	5.0.2	All	All	All
Application	Php	Php	5.0.3	All	All	All
Application	Php	Php	5.0.4	All	All	All
Application	Php	Php	5.0.5	All	All	All
Application	Php	Php	5.1.0	All	All	All
Application	Php	Php	5.1.1	All	All	All
Application	Php	Php	5.1.2	All	All	All
Application	Php	Php	5.1.3	All	All	All
Application	Php	Php	5.1.4	All	All	All
Application	Php	Php	5.1.5	All	All	All
Application	Php	Php	5.1.6	All	All	All
Application	Php	Php	5.2.0	All	All	All
Application	Php	Php	5.2.1	All	All	All
Application	Php	Php	5.4.0	All	All	All
Application	Php	Php	4.0	All	All	All
Application	Php	Php	4.0	beta1	All	All
Application	Php	Php	4.0	beta2	All	All
Application	Php	Php	4.0	beta3	All	All
Application	Php	Php	4.0	beta4	All	All
Application	Php	Php	4.0	beta_4_patch1	All	All
Application	Php	Php	4.0	rc1	All	All
Application	Php	Php	4.0	rc2	All	All
Application	Php	Php	4.0.0	All	All	All
Application	Php	Php	4.0.1	All	All	All
Application	Php	Php	4.0.1	patch1	All	All
Application	Php	Php	4.0.1	patch2	All	All
Application	Php	Php	4.0.2	All	All	All
Application	Php	Php	4.0.3	All	All	All
Application	Php	Php	4.0.3	patch1	All	All

Application	Php	Php	Node	Platform	Env	Env
Application	Php	Php	4.0.4	All	All	All
Application	Php	Php	4.0.4	patch1	All	All
Application	Php	Php	4.0.5	All	All	All
Application	Php	Php	4.0.6	All	All	All
Application	Php	Php	4.0.7	All	All	All
Application	Php	Php	4.0.7	rc1	All	All
Application	Php	Php	4.0.7	rc2	All	All
Application	Php	Php	4.0.7	rc3	All	All
Application	Php	Php	4.1.0	All	All	All
Application	Php	Php	4.1.1	All	All	All
Application	Php	Php	4.1.2	All	All	All
Application	Php	Php	4.2	All	dev	All
Application	Php	Php	4.2.0	All	All	All
Application	Php	Php	4.2.1	All	All	All
Application	Php	Php	4.2.2	All	All	All
Application	Php	Php	4.2.3	All	All	All
Application	Php	Php	4.3.0	All	All	All
Application	Php	Php	4.3.1	All	All	All
Application	Php	Php	4.3.10	All	All	All
Application	Php	Php	4.3.11	All	All	All
Application	Php	Php	4.3.2	All	All	All
Application	Php	Php	4.3.3	All	All	All
Application	Php	Php	4.3.4	All	All	All
Application	Php	Php	4.3.5	All	All	All
Application	Php	Php	4.3.6	All	All	All
Application	Php	Php	4.3.7	All	All	All
Application	Php	Php	4.3.8	All	All	All
Application	Php	Php	4.3.9	All	All	All
Application	Php	Php	4.4.0	All	All	All
Application	Php	Php	4.4.1	All	All	All
Application	Php	Php	4.4.2	All	All	All
Application	Php	Php	4.4.3	All	All	All
Application	Php	Php	4.4.4	All	All	All
Application	Php	Php	4.4.5	All	All	All
Application	Php	Php	4.4.6	All	All	All

cpe:2.3:a:php:php:4.0:rc2:*:*:*:*:*:
cpe:2.3:a:php:php:4.0.0:*:*:*:*:*:
cpe:2.3:a:php:php:4.0.1:*:*:*:*:*:
cpe:2.3:a:php:php:4.0.1:patch1:*:*:*:*:*:
cpe:2.3:a:php:php:4.0.1:patch2:*:*:*:*:*:
cpe:2.3:a:php:php:4.0.2:*:*:*:*:*:
cpe:2.3:a:php:php:4.0.3:*:*:*:*:*:
cpe:2.3:a:php:php:4.0.3:patch1:*:*:*:*:*:
cpe:2.3:a:php:php:4.0.4:*:*:*:*:*:
cpe:2.3:a:php:php:4.0.4:patch1:*:*:*:*:*:
cpe:2.3:a:php:php:4.0.5:*:*:*:*:*:
cpe:2.3:a:php:php:4.0.6:*:*:*:*:*:
cpe:2.3:a:php:php:4.0.7:*:*:*:*:*:
cpe:2.3:a:php:php:4.0.7:rc1:*:*:*:*:*:
cpe:2.3:a:php:php:4.0.7:rc2:*:*:*:*:*:
cpe:2.3:a:php:php:4.0.7:rc3:*:*:*:*:*:
cpe:2.3:a:php:php:4.1.0:*:*:*:*:*:
cpe:2.3:a:php:php:4.1.1:*:*:*:*:*:
cpe:2.3:a:php:php:4.1.2:*:*:*:*:*:
cpe:2.3:a:php:php:4.2:*:dev:*:*:*:*:
cpe:2.3:a:php:php:4.2.0:*:*:*:*:*:
cpe:2.3:a:php:php:4.2.1:*:*:*:*:*:
cpe:2.3:a:php:php:4.2.2:*:*:*:*:*:
cpe:2.3:a:php:php:4.2.3:*:*:*:*:*:
cpe:2.3:a:php:php:4.3.0:*:*:*:*:*:
cpe:2.3:a:php:php:4.3.1:*:*:*:*:*:
cpe:2.3:a:php:php:4.3.10:*:*:*:*:*:
cpe:2.3:a:php:php:4.3.11:*:*:*:*:*:
cpe:2.3:a:php:php:4.3.2:*:*:*:*:*:

cpe:2.3:a:php:php:4.3.3:*****:
cpe:2.3:a:php:php:4.3.4:*****:
cpe:2.3:a:php:php:4.3.5:*****:
cpe:2.3:a:php:php:4.3.6:*****:
cpe:2.3:a:php:php:4.3.7:*****:
cpe:2.3:a:php:php:4.3.8:*****:
cpe:2.3:a:php:php:4.3.9:*****:
cpe:2.3:a:php:php:4.4.0:*****:
cpe:2.3:a:php:php:4.4.1:*****:
cpe:2.3:a:php:php:4.4.2:*****:
cpe:2.3:a:php:php:4.4.3:*****:
cpe:2.3:a:php:php:4.4.4:*****:
cpe:2.3:a:php:php:4.4.5:*****:
cpe:2.3:a:php:php:4.4.6:*****:
cpe:2.3:a:php:php:5.0:rc1:*****:
cpe:2.3:a:php:php:5.0:rc2:*****:
cpe:2.3:a:php:php:5.0:rc3:*****:
cpe:2.3:a:php:php:5.0.0:*****:
cpe:2.3:a:php:php:5.0.0:beta1:*****:
cpe:2.3:a:php:php:5.0.0:beta2:*****:
cpe:2.3:a:php:php:5.0.0:beta3:*****:
cpe:2.3:a:php:php:5.0.0:beta4:*****:
cpe:2.3:a:php:php:5.0.0:rc1:*****:
cpe:2.3:a:php:php:5.0.0:rc2:*****:
cpe:2.3:a:php:php:5.0.0:rc3:*****:
cpe:2.3:a:php:php:5.0.1:*****:
cpe:2.3:a:php:php:5.0.2:*****:
cpe:2.3:a:php:php:5.0.3:*****:

cpe:2.3:a:php:php:5.0.4:*****:
cpe:2.3:a:php:php:5.0.5:*****:
cpe:2.3:a:php:php:5.1.0:*****:
cpe:2.3:a:php:php:5.1.1:*****:
cpe:2.3:a:php:php:5.1.2:*****:
cpe:2.3:a:php:php:5.1.3:*****:
cpe:2.3:a:php:php:5.1.4:*****:
cpe:2.3:a:php:php:5.1.5:*****:
cpe:2.3:a:php:php:5.1.6:*****:
cpe:2.3:a:php:php:5.2.0:*****:
cpe:2.3:a:php:php:5.2.1:*****:
cpe:2.3:a:php:php:5.4.0:*****:
cpe:2.3:a:php:php:4.0:*****:
cpe:2.3:a:php:php:4.0:beta1:*****:
cpe:2.3:a:php:php:4.0:beta2:*****:
cpe:2.3:a:php:php:4.0:beta3:*****:
cpe:2.3:a:php:php:4.0:beta4:*****:
cpe:2.3:a:php:php:4.0:beta_4_patch1:*****:
cpe:2.3:a:php:php:4.0:rc1:*****:
cpe:2.3:a:php:php:4.0:rc2:*****:
cpe:2.3:a:php:php:4.0.0:*****:
cpe:2.3:a:php:php:4.0.1:*****:
cpe:2.3:a:php:php:4.0.1:patch1:*****:
cpe:2.3:a:php:php:4.0.1:patch2:*****:
cpe:2.3:a:php:php:4.0.2:*****:
cpe:2.3:a:php:php:4.0.3:*****:
cpe:2.3:a:php:php:4.0.3:patch1:*****:
cpe:2.3:a:php:php:4.0.4:*****:
cpe:2.3:a:php:php:4.0.4:patch1:*****:

cpe:2.3:a:php:php:4.0.5:*:*:*:*:*:
cpe:2.3:a:php:php:4.0.6:*:*:*:*:*:
cpe:2.3:a:php:php:4.0.7:*:*:*:*:*:
cpe:2.3:a:php:php:4.0.7:rc1:*:*:*:*:*:
cpe:2.3:a:php:php:4.0.7:rc2:*:*:*:*:*:
cpe:2.3:a:php:php:4.0.7:rc3:*:*:*:*:*:
cpe:2.3:a:php:php:4.1.0:*:*:*:*:*:
cpe:2.3:a:php:php:4.1.1:*:*:*:*:*:
cpe:2.3:a:php:php:4.1.2:*:*:*:*:*:
cpe:2.3:a:php:php:4.2:*:*:*:*:*:dev:*:*:*:*:
cpe:2.3:a:php:php:4.2.0:*:*:*:*:*:
cpe:2.3:a:php:php:4.2.1:*:*:*:*:*:
cpe:2.3:a:php:php:4.2.2:*:*:*:*:*:
cpe:2.3:a:php:php:4.2.3:*:*:*:*:*:
cpe:2.3:a:php:php:4.3.0:*:*:*:*:*:
cpe:2.3:a:php:php:4.3.1:*:*:*:*:*:
cpe:2.3:a:php:php:4.3.10:*:*:*:*:*:
cpe:2.3:a:php:php:4.3.11:*:*:*:*:*:
cpe:2.3:a:php:php:4.3.2:*:*:*:*:*:
cpe:2.3:a:php:php:4.3.3:*:*:*:*:*:
cpe:2.3:a:php:php:4.3.4:*:*:*:*:*:
cpe:2.3:a:php:php:4.3.5:*:*:*:*:*:
cpe:2.3:a:php:php:4.3.6:*:*:*:*:*:
cpe:2.3:a:php:php:4.3.7:*:*:*:*:*:
cpe:2.3:a:php:php:4.3.8:*:*:*:*:*:
cpe:2.3:a:php:php:4.3.9:*:*:*:*:*:
cpe:2.3:a:php:php:4.4.0:*:*:*:*:*:
cpe:2.3:a:php:php:4.4.1:*:*:*:*:*:

cpe:2.3:a:php:php:4.4.2:*:*:*:*:*:
cpe:2.3:a:php:php:4.4.3:*:*:*:*:*:
cpe:2.3:a:php:php:4.4.4:*:*:*:*:*:
cpe:2.3:a:php:php:4.4.5:*:*:*:*:*:
cpe:2.3:a:php:php:4.4.6:*:*:*:*:*:
cpe:2.3:a:php:php:5.0:rc1:*:*:*:*:*:
cpe:2.3:a:php:php:5.0:rc2:*:*:*:*:*:
cpe:2.3:a:php:php:5.0:rc3:*:*:*:*:*:
cpe:2.3:a:php:php:5.0.0:*:*:*:*:*:
cpe:2.3:a:php:php:5.0.0:beta1:*:*:*:*:*:
cpe:2.3:a:php:php:5.0.0:beta2:*:*:*:*:*:
cpe:2.3:a:php:php:5.0.0:beta3:*:*:*:*:*:
cpe:2.3:a:php:php:5.0.0:beta4:*:*:*:*:*:
cpe:2.3:a:php:php:5.0.0:rc1:*:*:*:*:*:
cpe:2.3:a:php:php:5.0.0:rc2:*:*:*:*:*:
cpe:2.3:a:php:php:5.0.0:rc3:*:*:*:*:*:
cpe:2.3:a:php:php:5.0.1:*:*:*:*:*:
cpe:2.3:a:php:php:5.0.2:*:*:*:*:*:
cpe:2.3:a:php:php:5.0.3:*:*:*:*:*:
cpe:2.3:a:php:php:5.0.4:*:*:*:*:*:
cpe:2.3:a:php:php:5.0.5:*:*:*:*:*:
cpe:2.3:a:php:php:5.1.0:*:*:*:*:*:
cpe:2.3:a:php:php:5.1.1:*:*:*:*:*:
cpe:2.3:a:php:php:5.1.2:*:*:*:*:*:
cpe:2.3:a:php:php:5.1.3:*:*:*:*:*:
cpe:2.3:a:php:php:5.1.4:*:*:*:*:*:
cpe:2.3:a:php:php:5.1.5:*:*:*:*:*:
cpe:2.3:a:php:php:5.1.6:*:*:*:*:*:
cpe:2.3:a:php:php:5.2.0:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.1:*****:
cpe:2.3:a:php:php:5.4.0:*****:

← Previous ID

Next ID→

© CVE.report 2023  |

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](#)