



# CVE-2007-2519

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2007-2519
<b>State</b>	PUBLISHED
<b>Assigner</b>	mitre
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2007-05-22 19:30:00 UTC
<b>Updated</b>	2026-04-23 00:35:47 UTC
<b>Description</b>	Directory traversal vulnerability in the installer in PEAR 1.0 through 1.5.3 allows user-assisted remote attackers to overwrite

## Risk And Classification

**Primary CVSS:** v2.0 6.8 from nvd@nist.gov

AV:N/AC:M/Au:N/C:P/I:P/A:P

**Problem Types:** NVD-CWE-Other | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:M/Au:N/C:P/I:P/A:P

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Php Group	Pear	1.0	All	All	All

Application	Php Group	Pear	1.0.1	All	All	All
Application	Php Group	Pear	1.1	All	All	All
Application	Php Group	Pear	1.2	All	All	All
Application	Php Group	Pear	1.2.1	All	All	All
Application	Php Group	Pear	1.2b1	All	All	All
Application	Php Group	Pear	1.2b2	All	All	All
Application	Php Group	Pear	1.2b3	All	All	All
Application	Php Group	Pear	1.2b4	All	All	All
Application	Php Group	Pear	1.2b5	All	All	All
Application	Php Group	Pear	1.3	All	All	All
Application	Php Group	Pear	1.3.1	All	All	All
Application	Php Group	Pear	1.3.3	All	All	All
Application	Php Group	Pear	1.3.3.1	All	All	All
Application	Php Group	Pear	1.3.4	All	All	All
Application	Php Group	Pear	1.3.5	All	All	All
Application	Php Group	Pear	1.3.6	All	All	All
Application	Php Group	Pear	1.3b1	All	All	All
Application	Php Group	Pear	1.3b2	All	All	All
Application	Php Group	Pear	1.3b3	All	All	All
Application	Php Group	Pear	1.3b5	All	All	All
Application	Php Group	Pear	1.3b6	All	All	All
Application	Php Group	Pear	1.4.0	All	All	All
Application	Php Group	Pear	1.4.0a1	All	All	All
Application	Php Group	Pear	1.4.0a10	All	All	All
Application	Php Group	Pear	1.4.0a11	All	All	All
Application	Php Group	Pear	1.4.0a12	All	All	All
Application	Php Group	Pear	1.4.0a2	All	All	All
Application	Php Group	Pear	1.4.0a3	All	All	All
Application	Php Group	Pear	1.4.0a4	All	All	All
Application	Php Group	Pear	1.4.0a5	All	All	All
Application	Php Group	Pear	1.4.0a6	All	All	All
Application	Php Group	Pear	1.4.0a7	All	All	All
Application	Php Group	Pear	1.4.0a8	All	All	All
Application	Php Group	Pear	1.4.0a9	All	All	All
Application	Php Group	Pear	1.4.0b1	All	All	All
Application	Php Group	Pear	1.4.0b2	All	All	All

Application	<a href="#">Php Group</a>	<a href="#">Pear</a>	1.4.0rc1	All	All	All
Application	<a href="#">Php Group</a>	<a href="#">Pear</a>	1.4.0rc2	All	All	All
Application	<a href="#">Php Group</a>	<a href="#">Pear</a>	1.4.1	All	All	All
Application	<a href="#">Php Group</a>	<a href="#">Pear</a>	1.4.10	All	All	All
Application	<a href="#">Php Group</a>	<a href="#">Pear</a>	1.4.10rc1	All	All	All
Application	<a href="#">Php Group</a>	<a href="#">Pear</a>	1.4.11	All	All	All
Application	<a href="#">Php Group</a>	<a href="#">Pear</a>	1.4.2	All	All	All
Application	<a href="#">Php Group</a>	<a href="#">Pear</a>	1.4.3	All	All	All
Application	<a href="#">Php Group</a>	<a href="#">Pear</a>	1.4.4	All	All	All
Application	<a href="#">Php Group</a>	<a href="#">Pear</a>	1.4.5	All	All	All
Application	<a href="#">Php Group</a>	<a href="#">Pear</a>	1.4.6	All	All	All
Application	<a href="#">Php Group</a>	<a href="#">Pear</a>	1.4.7	All	All	All
Application	<a href="#">Php Group</a>	<a href="#">Pear</a>	1.4.8	All	All	All
Application	<a href="#">Php Group</a>	<a href="#">Pear</a>	1.4.9	All	All	All
Application	<a href="#">Php Group</a>	<a href="#">Pear</a>	1.5.0	All	All	All
Application	<a href="#">Php Group</a>	<a href="#">Pear</a>	1.5.0a1	All	All	All
Application	<a href="#">Php Group</a>	<a href="#">Pear</a>	1.5.0rc1	All	All	All
Application	<a href="#">Php Group</a>	<a href="#">Pear</a>	1.5.0rc2	All	All	All
Application	<a href="#">Php Group</a>	<a href="#">Pear</a>	1.5.0rc3	All	All	All
Application	<a href="#">Php Group</a>	<a href="#">Pear</a>	1.5.1	All	All	All
Application	<a href="#">Php Group</a>	<a href="#">Pear</a>	1.5.2	All	All	All
Application	<a href="#">Php Group</a>	<a href="#">Pear</a>	1.5.3	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

### References

Reference	Source	Link
Support / Security / Advisories // MDKSA-2007:110   Mandriva	af854a3a-2127-422b-91ae-364da2661108	<a href="http://www.mandriva.com">www.mandriva.com</a>
Ubuntu update for php - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108	<a href="http://secunia.com">secunia.com</a>
PHP PEAR INSTALL-AS Attribute Arbitrary File Overwrite Vulnerability	af854a3a-2127-422b-91ae-364da2661108	<a href="http://www.securityfocus.com">www.securityfocus.com</a>
pear.php.net/advisory-20070507.txt	af854a3a-2127-422b-91ae-364da2661108	<a href="http://pear.php.net">pear.php.net</a>
PEAR :: Arbitrary File Overwrite Vulnerability in the PEAR Installer	af854a3a-2127-422b-91ae-364da2661108	<a href="http://pear.php.net">pear.php.net</a>
osvdb.org/42108	af854a3a-2127-422b-91ae-364da2661108	<a href="http://osvdb.org">osvdb.org</a>
USN-462-1: PHP vulnerabilities   Ubuntu	af854a3a-2127-422b-91ae-364da2661108	<a href="http://www.ubuntu.com">www.ubuntu.com</a>

Webmail- OVH	af854a3a-2127-422b-91ae-364da2661108	<a href="http://www.vupen.com">www.vupen.com</a>
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108	<a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

### Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-05-24	Mark J Cox	Installation of a PEAR package from an untrusted source could allow malicious code to be installed.

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

© [CVE.report](http://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](http://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://MITRE's CVE web site). This site includes MITRE data granted under the following [license](http://license).

Free CVE JSON API [cve.report/api](http://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](http://status.cve.report)