



# CVE-2004-1065

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

## Summary

<b>CVE</b>	CVE-2004-1065
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2005-01-10 05:00:00 UTC
<b>Updated</b>	2018-10-30 16:25:00 UTC
<b>Description</b>	Buffer overflow in the exif_read_data function in PHP before 4.3.10 and PHP 5.x up to 5.0.2 allows remote attackers to exe

## Risk And Classification

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

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Openpkg</a>	<a href="#">Openpkg</a>	2.1	All	All	All
Application	<a href="#">Openpkg</a>	<a href="#">Openpkg</a>	2.2	All	All	All
Application	<a href="#">Openpkg</a>	<a href="#">Openpkg</a>	current	All	All	All
Application	<a href="#">Openpkg</a>	<a href="#">Openpkg</a>	2.1	All	All	All
Application	<a href="#">Openpkg</a>	<a href="#">Openpkg</a>	2.2	All	All	All
Application	<a href="#">Openpkg</a>	<a href="#">Openpkg</a>	current	All	All	All
Application	<a href="#">Php</a>	<a href="#">Php</a>	3.0	All	All	All
Application	<a href="#">Php</a>	<a href="#">Php</a>	3.0.1	All	All	All
Application	<a href="#">Php</a>	<a href="#">Php</a>	3.0.10	All	All	All
Application	<a href="#">Php</a>	<a href="#">Php</a>	3.0.11	All	All	All
Application	<a href="#">Php</a>	<a href="#">Php</a>	3.0.12	All	All	All
Application	<a href="#">Php</a>	<a href="#">Php</a>	3.0.13	All	All	All
Application	<a href="#">Php</a>	<a href="#">Php</a>	3.0.14	All	All	All
Application	<a href="#">Php</a>	<a href="#">Php</a>	3.0.15	All	All	All
Application	<a href="#">Php</a>	<a href="#">Php</a>	3.0.16	All	All	All
Application	<a href="#">Php</a>	<a href="#">Php</a>	3.0.17	All	All	All
Application	<a href="#">Php</a>	<a href="#">Php</a>	3.0.18	All	All	All

Application	Php	Php	3.0.2	All	All	All
Application	Php	Php	3.0.3	All	All	All
Application	Php	Php	3.0.4	All	All	All
Application	Php	Php	3.0.5	All	All	All
Application	Php	Php	3.0.6	All	All	All
Application	Php	Php	3.0.7	All	All	All
Application	Php	Php	3.0.8	All	All	All
Application	Php	Php	3.0.9	All	All	All
Application	Php	Php	4.0	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	4.0.5	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	4.3.2	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	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	5.0.1	All	All	All
Application	Php	Php	5.0.2	All	All	All
Application	Php	Php	3.0	All	All	All
Application	Php	Php	3.0.1	All	All	All
Application	Php	Php	3.0.10	All	All	All
Application	Php	Php	3.0.11	All	All	All
Application	Php	Php	3.0.12	All	All	All
Application	Php	Php	3.0.13	All	All	All
Application	Php	Php	3.0.14	All	All	All
Application	Php	Php	3.0.15	All	All	All
Application	Php	Php	3.0.16	All	All	All
Application	Php	Php	3.0.17	All	All	All
Application	Php	Php	3.0.18	All	All	All
Application	Php	Php	3.0.2	All	All	All
Application	Php	Php	3.0.3	All	All	All
Application	Php	Php	3.0.4	All	All	All
Application	Php	Php	3.0.5	All	All	All
Application	Php	Php	3.0.6	All	All	All
Application	Php	Php	3.0.7	All	All	All
Application	Php	Php	3.0.8	All	All	All
Application	Php	Php	3.0.9	All	All	All
Application	Php	Php	4.0	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	4.0.5	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	4.3.2	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	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	5.0.1	All	All	All
Application	Php	Php	5.0.2	All	All	All
Operating System	Trustix	Secure Linux	2.0	All	All	All
Operating System	Trustix	Secure Linux	2.1	All	All	All
Operating System	Trustix	Secure Linux	2.2	All	All	All

Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	2.0	All	All	All
Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	2.1	All	All	All
Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	2.2	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	Source	Link	Tags
Security Announcement	SUSE	<a href="http://www.novell.com">www.novell.com</a>	
redhat.com   Red Hat Support	REDHAT	<a href="http://www.redhat.com">www.redhat.com</a>	
IBM X-Force Exchange	XF	<a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>	
HPSBMA01212	HP	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	
OpenPKG-SA-2004.053	OPENPKG	<a href="http://msgs.securepoint.com">msgs.securepoint.com</a>	
Advisories - Mandriva	MANDRAKE	<a href="http://www.mandriva.com">www.mandriva.com</a>	
PHP: PHP 4.3.10 Release Announcement	CONFIRM	<a href="http://www.php.net">www.php.net</a>	
FLSA:2344	FEDORA	<a href="http://bugzilla.fedora.us">bugzilla.fedora.us</a>	
Repository / Oval Repository	OVAL	<a href="http://oval.cisecurity.org">oval.cisecurity.org</a>	
redhat.com   Red Hat Support	REDHAT	<a href="http://www.redhat.com">www.redhat.com</a>	Patch, Vendor Advisory
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

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](http://status.cve.report)