



CVE-2006-4433

Published on: 08/28/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:57 PM UTC

CVE-2006-4433

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

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

PHP before 4.4.3 and 5.x before 5.1.4 does not limit the character set of the session identifier (PHPSESSID) for third party session handlers, which might make it easier for remote attackers to exploit other vulnerabilities by inserting PHP code into the PHPSESSID, which is stored in the session file. NOTE: it could be argued that this not a vulnerability in PHP itself, rather a design limitation that enables certain attacks against session handlers that do not account for this limitation.

CVE-2006-4433 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
No Description Provided	www.osvdb.org	OSVDB 28273
	Inactive Link Not Archived	
SecurityReason - Zend Platform Multiple Remote Vulnerabilities	securityreason.com text/html	SREASON 1466
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2006-3388
Zend Platform Multiple Vulnerabilities - Advisories - Secunia	Patch Vendor Advisory web.archive.org text/html	SECUNIA 21573

Hardened-PHP Project - PhP Security - Advisory
05/2006

Patch
Vendor Advisory
www.hardened-php.net
text/html

MISC www.hardened-php.net/advisory_052006.128.html

No Description Provided

www.osvdb.org

OSVDB 28233

Inactive Link Not Archived

SecurityFocus

www.securityfocus.com
text/html

BUGTRAQ 20060824 Advisory 05/2006: Zend Platform
Multiple Remote Vulnerabilities

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	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	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	Phn	Phn	4.2	All	dev	All

Application	Php	Php	PHP	PHP	OS	Arch
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	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
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: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: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: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:*****:

[← 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](#)