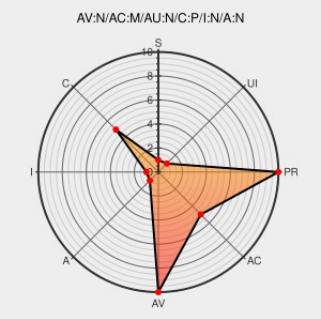
CVE-2007-5899

Published on: 11/20/2007 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:38 PM UTC

CVE-2007-5899

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Php from Php contain the following vulnerability:

The output_add_rewrite_var function in PHP before 5.2.5 rewrites local forms in which the ACTION attribute references a non-local URL, which allows remote attackers to obtain potentially sensitive information by reading the requests for this URL, as demonstrated by a rewritten form containing a local session ID.

CVE-2007-5899 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
PHP Bugs: #42869: URL rewrite mechanism - data sent to foreign sites	bugs.php.net text/html	CONFIRM bugs.php.net/bug.php?id=42869
PHP: PHP 5 ChangeLog	www.php.net text/html	CONFIRM www.php.net/ChangeLog-5.php#5.2.5
USN-628-1: PHP vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-628-1
Fedora update for php - Secunia Advisories - Vulnerability Intelligence - Secunia.com	web.archive.org text/html	SECUNIA 30828
Ubuntu update for php - Advisories - Secunia	web.archive.org text/html	SECUNIA 27864
USN-549-2: PHP regression | Ubuntu	www.ubuntu.com	UBUNTU USN-549-2

	text/html	
No Description Provided	osvdb.org Inactive Link Not Archived	OSVDB 38918
rhn.redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2008:0545
Debian -- Security Information -- DSA-1444-2 php5	www.debian.org Depreciated Link text/html	DEBIAN DSA-1444
About Secunia Research | Flexera	web.archive.org text/html	SECUNIA 31200
Advisories | Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2008:126
rhn.redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2008:0582
Advisories | Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2008:127
HP-UX update for Apache with PHP - Advisories - Secunia	web.archive.org text/html	SECUNIA 30040
Advisories | Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2008:125
PHP: PHP 5.2.5 Release Announcement	www.php.net text/html	CONFIRM www.php.net/releases/5_2_5.php
No Description Provided	issues.rpath.com Inactive Link Not Archived	CONFIRM issues.rpath.com/browse/RPL-1943
Red Hat update for php - Secunia Advisories - Vulnerability Intelligence - Secunia.com	web.archive.org text/html	SECUNIA 31119
SecurityFocus	www.securityfocus.com text/html	HP SSRT080056
Bug #173043 “php5 5.2.3-1ubuntu6.1 introduced segfault regressio...” : Bugs : “php5” package : Ubuntu	launchpad.net text/html	CONFIRM launchpad.net/bugs/173043
Red Hat update for php - Secunia Advisories - Vulnerability Intelligence - Secunia.com	web.archive.org text/html	SECUNIA 31124
Debian update for php5 - Advisories - Secunia	web.archive.org text/html	SECUNIA 28249
USN-549-1: PHP vulnerabilities | Ubuntu security notices	usn.ubuntu.com text/html	UBUNTU USN-549-1
Advisories:rPSA-2007-0242 - rPath Wiki	web.archive.org text/html Inactive Link Not Archived	CONFIRM wiki.rpath.com/wiki/Advisories:rPSA-2007-0242
rhn.redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2008:0546
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:11211
rhn.redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2008:0544

[SECURITY] Fedora 8 Update: php-5.2.6-2.fc8	www.redhat.com text/html	FEDORA FEDORA-2008-3864
rhn.redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2008:0505
rPath update for php5 - Advisories - Secunia	web.archive.org text/html	SECUNIA 27659

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	All	All	All	All

cpe:2.3:a:php:php:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← 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 registred 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