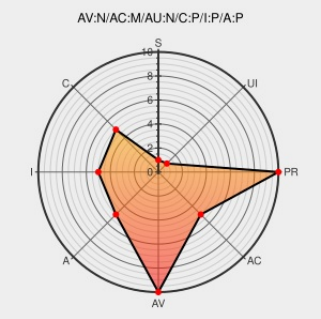
CVE-2010-2950

Published on: 09/28/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:10 PM UTC

CVE-2010-2950

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



Certain versions of Php from Php contain the following vulnerability:

Format string vulnerability in stream.c in the phar extension in PHP 5.3.x through 5.3.3 allows context-dependent attackers to obtain sensitive information (memory contents) and possibly execute arbitrary code via a crafted phar:// URI that is not properly handled by the phar_stream_flush function, leading to errors in the php_stream_wrapper_log_error function. NOTE: this vulnerability exists because of an incomplete fix for CVE-2010-2094.

CVE-2010-2950 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
APPLE-SA-2011-03-21-1 Mac OS X v10.6.7 and Security Update 2011-001	lists.apple.com text/html	APPLE APPLE-SA-2011-03-21-1
Bug 598537 – CVE-2010-2094 php: Multiple format string flaws in the phar extension (MOPS-2010-025 MOPS-2010-026 MOPS-2010-027 MOPS-2010-028)	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=598537
[security-announce] SUSE Security Summary Report: SUSE-SR:2010:017	Exploit lists.opensuse.org text/html	SUSE SUSE-SR:2010:017
'[security bulletin] HPSBMA02662 SSRT100409 rev.1 - HP System Management Homepage (SMH) for Linux and' - MARC	marc.info text/html	HP HPSBMA02662

PHP: PHP 5.3.4 Release Announcement	www.php.net text/html	CONFIRM www.php.net/releases/5_3_4.php
PHP: Revision 302565	svn.php.net text/html	CONFIRM svn.php.net/viewvc?view=revision&revision=302565
Support / Security / Advisories / / MDVSA-2010:254 | Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2010:254
About the security content of Mac OS X v10.6.7 and Security Update 2011-001	support.apple.com text/html	CONFIRM support.apple.com/kb/HT4581
CVE-2010-2950	security-tracker.debian.org text/html	CONFIRM security-tracker.debian.org/tracker/CVE-2010-2950
PHP: PHP 5 ChangeLog	www.php.net text/html	CONFIRM www.php.net/ChangeLog-5.php
PHP: News Archive - 2010	www.php.net text/html	CONFIRM www.php.net/archive/2010.php#id2010-12-10-1
MOPS-2010-024: PHP phar_stream_flush Format String Vulnerability « the Month of PHP Security	web.archive.org text/html Inactive Link Not Archived	MISC php-security.org/2010/05/14/mops-2010-024-php-phar_stream_flush-format-string-vulnerability/index.html

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	5.3.0	All	All	All
Application	Php	Php	5.3.1	All	All	All
Application	Php	Php	5.3.2	All	All	All
Application	Php	Php	5.3.3	All	All	All
Application	Php	Php	5.3.0	All	All	All
Application	Php	Php	5.3.1	All	All	All
Application	Php	Php	5.3.2	All	All	All
Application	Php	Php	5.3.3	All	All	All

cpe:2.3:a:php:php:5.3.0:*:*:*:*:*:*:*

cpe:2.3:a:php:php:5.3.1:*:*:*:*:*:*:*

cpe:2.3:a:php:php:5.3.2:*:*:*:*:*:*:*

cpe:2.3:a:php:php:5.3.3:*:*:*:*:*:*:*

cpe:2.3:a:php:php:5.3.0:*:*:*:*:*:*:*

cpe:2.3:a:php:php:5.3.1:*:*:*:*:*:*:*

cpe:2.3:a:php:php:5.3.2:*:*:*:*:*:*:*

cpe:2.3:a:php:php:5.3.3:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→