

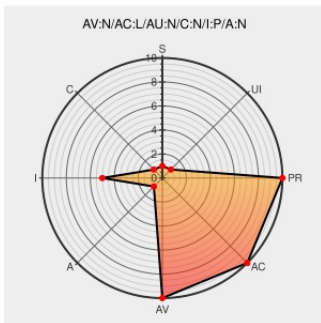


CVE-2009-3557

Published on: 11/23/2009 12:00:00 AM UTC

Last Modified on: 02/13/2023 02:10:38 AM UTC

CVE-2009-3557

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

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

The tempnam function in ext/standard/file.c in PHP before 5.2.12 and 5.3.x before 5.3.1 allows context-dependent attackers to bypass safe_mode restrictions, and create files in group-writable or world-writable directories, via the dir and prefix arguments.

CVE-2009-3557 has been assigned by [secalert@redhat.com](#) to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

PHP: PHP 5.2.12 Release Announcement

[www.php.net](#)
[text/html](#)

[php](#) CONFIRM
[www.php.net/releases/5_2_12.php](#)

oss-security - Re: CVE request: php 5.3.1 update

[Patch](#)
[www.openwall.com](#)
[text/html](#)

[MLIST \[oss-security\] 20091120 Re: CVE request: php 5.3.1 update](#)

PHP: PHP 5.3.1 Release Announcement

[Patch](#)
[Vendor Advisory](#)
[www.php.net](#)
[text/html](#)

[php](#) CONFIRM
[www.php.net/releases/5_3_1.php](#)

HP-UX update for Apache with PHP - Advisories - Community

[web.archive.org](#)
[text/html](#)

[X](#) SECUNIA 40262

PHP Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com

[web.archive.org](#)
[text/html](#)

[X](#) SECUNIA 37821

Webmail : Solution de messagerie professionnelle - OVHcloud-OVH	www.vupen.com text/html	VUPEN ADV-2009-3593
'[security bulletin] HPSBUX02543 SSRT100152 rev.1 - HP-UX Running Apache with PHP, Remote Denial of S' - MARC	marc.info text/html	HP SSRT100152
PHP 5.2.11 tempnam() safe_mode bypass - SecurityReason.com	Exploit securityreason.com text/html	SREASON 6601
APPLE-SA-2010-03-29-1 Security Update 2010-002 / Mac OS X v10.6.3	lists.apple.com text/html	APPLE APPLE-SA-2010-03-29-1
PHP Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	Vendor Advisory web.archive.org text/html	SECUNIA 37412
oss-security - CVE request: php 5.3.1 update	Patch www.openwall.com text/html	MLIST [oss-security] 20091120 CVE request: php 5.3.1 update
ViewVC Exception	svn.php.net text/html Inactive Link Not Archived	CONFIRM svn.php.net/viewvc/php/php-src/branches/PHP_5_2/ext/standard/file.c?view=log
php.announce: 5.3.1 Release announcement	news.php.net text/xml	MLIST [php-announce] 20091119 5.3.1 Release announcement
ViewVC Exception	svn.php.net text/html Inactive Link Not Archived	CONFIRM svn.php.net/viewvc/php/php-src/branches/PHP_5_3/ext/standard/file.c?view=log
PHP: Revision 288945	svn.php.net text/html	CONFIRM svn.php.net/viewvc?view=revision&revision=288945
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:7396
Support / Security / Advisories // MDVSA-2009:285 Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2009:285
PHP: PHP 5 ChangeLog	Patch Vendor Advisory www.php.net text/html	CONFIRM www.php.net/ChangeLog-5.php
About the security content of Security Update 2010-002 / Mac OS X v10.6.3	support.apple.com text/html	CONFIRM support.apple.com/kb/HT4077
Support / Security / Advisories // MDVSA-2009:302 Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2009:302
oss-security - Re: CVE request: php 5.3.1 update	Patch www.openwall.com text/html	MLIST [oss-security] 20091120 Re: CVE request: php 5.3.1 update
Support / Security / Advisories // MDVSA-2009:303 Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2009:303

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	1.0	All	All	All
Application	Php	Php	2.0	All	All	All
Application	Php	Php	2.0b10	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	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	4.0.0	All	All	All
Application	Php	Php	4.0.1	All	All	All
Application	Php	Php	4.0.2	All	All	All

Application	Php	Php	4.0.3	All	All	All
Application	Php	Php	4.0.4	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	4.1.0	All	All	All
Application	Php	Php	4.1.1	All	All	All
Application	Php	Php	4.1.2	All	All	All
Application	Php	Php	4.2.0	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	4.3.7	All	All	All
Application	Php	Php	4.4.2	All	All	All
Application	Php	Php	4.4.7	All	All	All
Application	Php	Php	4.4.8	All	All	All
Application	Php	Php	4.4.9	All	All	All
Application	Php	Php	5.0.0	All	All	All
Application	Php	Php	5.0.0	beta4	All	All
Application	Php	Php	5.0.3	All	All	All
Application	Php	Php	5.1.1	All	All	All
Application	Php	Php	5.2.1	All	All	All
Application	Php	Php	5.2.10	All	All	All
Application	Php	Php	5.2.5	All	All	All
Application	Php	Php	5.2.6	All	All	All
Application	Php	Php	5.3.0	All	All	All
Application	Php	Php	1.0	All	All	All
Application	Php	Php	2.0	All	All	All
Application	Php	Php	2.0b10	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	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	4.0.0	All	All	All
Application	Php	Php	4.0.1	All	All	All
Application	Php	Php	4.0.2	All	All	All
Application	Php	Php	4.0.3	All	All	All
Application	Php	Php	4.0.4	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	4.1.0	All	All	All
Application	Php	Php	4.1.1	All	All	All
Application	Php	Php	4.1.2	All	All	All
Application	Php	Php	4.2.0	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	4.3.7	All	All	All
Application	Php	Php	4.4.2	All	All	All
Application	Php	Php	4.4.7	All	All	All
Application	Php	Php	4.4.8	All	All	All
Application	Php	Php	4.4.9	All	All	All
Application	Php	Php	5.0.0	All	All	All
Application	Php	Php	5.0.0	beta4	All	All
Application	Php	Php	5.0.3	All	All	All
Application	Php	Php	5.1.1	All	All	All
Application	Php	Php	5.2.1	All	All	All
Application	Php	Php	5.2.10	All	All	All
Application	Php	Php	5.2.5	All	All	All
Application	Php	Php	5.2.6	All	All	All
Application	Php	Php	5.3.0	All	All	All
Application	Php	Php	All	All	All	All
cpe:2.3:a:php:php:1.0:*****:						
cpe:2.3:a:php:php:2.0:*****:						
cpe:2.3:a:php:php:2.0b10:*****:						
cpe:2.3:a:php:php:3.0:*****:						
cpe:2.3:a:php:php:3.0.1:*****:						
cpe:2.3:a:php:php:3.0.10:*****:						
cpe:2.3:a:php:php:3.0.11:*****:						
cpe:2.3:a:php:php:3.0.12:*****:						
cpe:2.3:a:php:php:3.0.13:*****:						
cpe:2.3:a:php:php:3.0.14:*****:						

cpe:2.3:a:php:php:3.0.15:*****:
cpe:2.3:a:php:php:3.0.16:*****:
cpe:2.3:a:php:php:3.0.17:*****:
cpe:2.3:a:php:php:3.0.18:*****:
cpe:2.3:a:php:php:3.0.2:*****:
cpe:2.3:a:php:php:3.0.3:*****:
cpe:2.3:a:php:php:3.0.4:*****:
cpe:2.3:a:php:php:3.0.5:*****:
cpe:2.3:a:php:php:3.0.6:*****:
cpe:2.3:a:php:php:3.0.7:*****:
cpe:2.3:a:php:php:3.0.8:*****:
cpe:2.3:a:php:php:3.0.9:*****:
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:4.0.0:*****:
cpe:2.3:a:php:php:4.0.1:*****:
cpe:2.3:a:php:php:4.0.2:*****:
cpe:2.3:a:php:php:4.0.3:*****:
cpe:2.3:a:php:php:4.0.4:*****:
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:4.1.0:*****:
cpe:2.3:a:php:php:4.1.1:*****:

cpe:2.3:a:php:php:4.1.2:*****:
cpe:2.3:a:php:php:4.2.0:*****:
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:4.3.7:*****:
cpe:2.3:a:php:php:4.4.2:*****:
cpe:2.3:a:php:php:4.4.7:*****:
cpe:2.3:a:php:php:4.4.8:*****:
cpe:2.3:a:php:php:4.4.9:*****:
cpe:2.3:a:php:php:5.0.0:*****:
cpe:2.3:a:php:php:5.0.0:beta4:*****:
cpe:2.3:a:php:php:5.0.3:*****:
cpe:2.3:a:php:php:5.1.1:*****:
cpe:2.3:a:php:php:5.2.1:*****:
cpe:2.3:a:php:php:5.2.10:*****:
cpe:2.3:a:php:php:5.2.5:*****:
cpe:2.3:a:php:php:5.2.6:*****:
cpe:2.3:a:php:php:5.3.0:*****:
cpe:2.3:a:php:php:1.0:*****:
cpe:2.3:a:php:php:2.0:*****:
cpe:2.3:a:php:php:2.0b10:*****:
cpe:2.3:a:php:php:3.0:*****:
cpe:2.3:a:php:php:3.0.1:*****:

cpe:2.3:a:php:php:3.0.1:~::~::~:
cpe:2.3:a:php:php:3.0.10:~::~::~:
cpe:2.3:a:php:php:3.0.11:~::~::~:
cpe:2.3:a:php:php:3.0.12:~::~::~:
cpe:2.3:a:php:php:3.0.13:~::~::~:
cpe:2.3:a:php:php:3.0.14:~::~::~:
cpe:2.3:a:php:php:3.0.15:~::~::~:
cpe:2.3:a:php:php:3.0.16:~::~::~:
cpe:2.3:a:php:php:3.0.17:~::~::~:
cpe:2.3:a:php:php:3.0.18:~::~::~:
cpe:2.3:a:php:php:3.0.2:~::~::~:
cpe:2.3:a:php:php:3.0.3:~::~::~:
cpe:2.3:a:php:php:3.0.4:~::~::~:
cpe:2.3:a:php:php:3.0.5:~::~::~:
cpe:2.3:a:php:php:3.0.6:~::~::~:
cpe:2.3:a:php:php:3.0.7:~::~::~:
cpe:2.3:a:php:php:3.0.8:~::~::~:
cpe:2.3:a:php:php:3.0.9:~::~::~:
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:4.0.0:~::~::~:
cpe:2.3:a:php:php:4.0.1:~::~::~:
cpe:2.3:a:php:php:4.0.2:~::~::~:
cpe:2.3:a:php:php:4.0.3:~::~::~:
cpe:2.3:a:php:php:4.0.4:~::~::~:

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:4.1.0:*****:
cpe:2.3:a:php:php:4.1.1:*****:
cpe:2.3:a:php:php:4.1.2:*****:
cpe:2.3:a:php:php:4.2.0:*****:
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:4.3.7:*****:
cpe:2.3:a:php:php:4.4.2:*****:
cpe:2.3:a:php:php:4.4.7:*****:
cpe:2.3:a:php:php:4.4.8:*****:
cpe:2.3:a:php:php:4.4.9:*****:
cpe:2.3:a:php:php:5.0.0:*****:
cpe:2.3:a:php:php:5.0.0:beta4:*****:
cpe:2.3:a:php:php:5.0.3:*****:
cpe:2.3:a:php:php:5.1.1:*****:
cpe:2.3:a:php:php:5.2.1:*****:
cpe:2.3:a:php:php:5.2.10:*****:
cpe:2.3:a:php:php:5.2.5:*****:
cpe:2.3:a:php:php:5.2.6:*****:

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

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

[← 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](#)