



CVE-2006-1494

Published on: 04/10/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:59 PM UTC

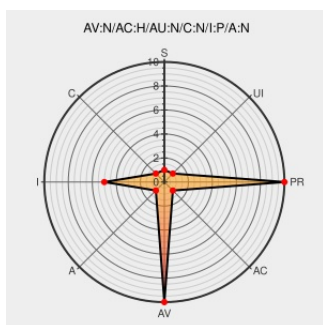
CVE-2006-1494

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Directory traversal vulnerability in file.c in PHP 4.4.2 and 5.1.2 allows local users to bypass open_basedir restrictions allows remote attackers to create files in arbitrary directories via the tempnam function.

CVE-2006-1494 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **2.6 - LOW**

Access
Vector

NETWORK

Access
Complexity

HIGH

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

PHP tempname() Argument Error Lets Users Bypass open_basedir Restrictions - SecurityTracker

[securitytracker.com](#)
text/html

[SECTRAK 1015881](#)

Repository / Oval Repository

[oval.cisecurity.org](#)
text/html

[OVAL oval:org.mitre.oval:def:10196](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
text/html

[XF php-tempnam-directory-traversal\(25705\)](#)

SecurityFocus

[www.securityfocus.com](#)
text/html

[BUGTRAQ 20061005 rPSA-2006-0182-1 php php-mysql php-pgsql](#)

Ubuntu update for PHP - Advisories - Secunia

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

[SECUNIA 21125](#)

Avaya Products PHP Multiple Vulnerabilities - Advisories - Secunia

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

[SECUNIA 21723](#)

SecurityReason - tempnam() open_basedir bypass PHP 4.4.2 and 5.1.2	securityreason.com text/html	 SREASON 677
access.redhat.com	www.redhat.com text/html	 REDHAT RHSA-2006:0567
Red Hat update for php - Advisories - Secunia	web.archive.org text/html	 SECUNIA 21202
usn/usn-320-1 - Ubuntu: Linux for human beings	www.ubuntu.com text/html	 UBUNTU USN-320-1
Red Hat update for php - Advisories - Secunia	web.archive.org text/html	 SECUNIA 21031
Red Hat Stronghold updates for uw-imap and PHP - Advisories - Secunia	web.archive.org text/html	 SECUNIA 21252
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	 VUPEN ADV-2006-1290
rPath update for php - Advisories - Secunia	web.archive.org text/html	 SECUNIA 22225
PHP Multiple Safe_Mode and Open_Basedir Restriction Bypass Vulnerabilities	cve.report (archive) text/html	 BID 17439
Secunia - Advisories - SUSE updates for php4 / php5	web.archive.org text/html	 SECUNIA 19979
SGI Advanced Linux Environment Multiple Updates - Advisories - Secunia	web.archive.org text/html	 SECUNIA 21135
Security Announcement	web.archive.org text/html Inactive Link Not Archived	 SUSE SUSE-SA:2006:024
rhn.redhat.com Red Hat Support	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2006:0549
Advisories - Mandriva Linux	www.mandriva.com text/html	 MANDRIVA MDKSA-2006:074
No Description Provided	patches.sgi.com Inactive Link Not Archived	 SGI 20060701-01-U
PHP "phpinfo()" Cross-Site Scripting and Security Bypass - Advisories - Secunia	Exploit Patch Vendor Advisory web.archive.org text/html	 SECUNIA 19599
SecurityReason - tempnam() open_basedir bypass PHP 4.4.2 and 5.1.2	Exploit Patch securityreason.com text/html	 SREASONRES 20060408 tempnam() open_basedir bypass PHP 4.4.2 and 5.1.2
[#RPL-683] Multiple Vulnerabilities in PHP CVE-2006-1494 CVE-2006-1990 CVE-2006-3016 CVE-2006-3017 CVE-2006-4482 CVE-2006-4484 CVE-2006-4486 - rPath JIRA	web.archive.org text/html Inactive Link Not Archived	 CONFIRM issues.rpath.com/browse/RPL-683
ASA-2006-175 (RHSA-2006-0568)	support.avaya.com text/html	 CONFIRM support.avaya.com/elmodocs2/security/ASA-2006-175.htm
Multiple Vulnerabilities in PHP CVE-2006-1494 CVE-2006-1990 CVE-2006-3016 CVE-2006-3017 CVE-2006-4482 CVE-2006-4484 CVE-2006-4486 - rPath JIRA	web.archive.org text/html Inactive Link Not Archived	 SECUNIA 19599

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	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

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:5.0.1:*:*:*:*:*:
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:rc4:*:*:*:*:*:

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 →](#)