



# CVE-2005-3319

Published on: 10/27/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:23 PM UTC

## CVE-2005-3319

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

The apache2handler SAPI (sapi\_apache2.c) in the Apache module (mod\_php) for PHP 5.x before 5.1.0 final and 4.4 before 4.4.1 final allows attackers to cause a denial of service (segmentation fault) via the session.save\_path option in a .htaccess file or VirtualHost.

CVE-2005-3319 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **2.1 - LOW**

**Access Vector**

**LOCAL**

**Access Complexity**

**LOW**

**Authentication**

**NONE**

**Confidentiality Impact**

**NONE**

**Integrity Impact**

**NONE**

**Availability Impact**

**PARTIAL**

## CVE References

**Description**

**Tags**

**Link**

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

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

[VUPEN ADV-2006-4320](#)

Mac OS X Security Update Fixes Multiple Vulnerabilities - Advisories - Secunia

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

[SECUNIA 19064](#)

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

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

[VUPEN ADV-2006-0791](#)

SecurityReason

[securityreason.com](#)  
[text/html](#)

[SREASON 525](#)

IBM X-Force Exchange

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

[XF php-htaccess-dos\(22844\)](#)

IT Resource Center - login / register

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

[HP SSRT061238](#)

Inactive Link Not Archived

Gentoo Bug 107602 - dev-php/mod\_php: Local DoS through session.save\_path option

bugs.gentoo.org  
text/html

CONFIRM  
bugs.gentoo.org/show\_bug.cgi?id=107602

Advisories - Mandriva

www.mandriva.com  
text/html

MANDRIVA MDKSA-2005:213

PHP Apache 2 Local Denial of Service Vulnerability

cve.report (archive)  
text/html

BID 15177

APPLE-SA-2006-03-01 Security Update 2006-001

lists.apple.com  
text/html

APPLE APPLE-SA-2006-03-01

No Description Provided

web.archive.org  
text/html  
Inactive Link Not Archived

FULLDISC 20051024 php < 4.4.1 htaccess apache dos

HP System Management Homepage PHP Multiple Vulnerabilities - Advisories - Secunia

web.archive.org  
text/html

SECUNIA 22691

Apple Mac OS X Security Update 2006-001 Multiple Vulnerabilities

cve.report (archive)  
text/html

BID 16907

usn/usn-232-1 - Ubuntu Linux

www.ubuntu.com  
text/html

UBUNTU USN-232-1

Secunia - Advisories - Gentoo update for php

web.archive.org  
text/html

SECUNIA 17510

'php < 4.4.1 htaccess apache dos' - MARC

marc.info  
text/html

BUGTRAQ 20051024 php < 4.4.1 htaccess apache dos

Secunia - Advisories - Ubuntu update for php4/php5

web.archive.org  
text/html

SECUNIA 18198

Gentoo Linux Documentation -- PHP: Multiple vulnerabilities

www.gentoo.org  
text/html

GENTOO GLSA-200511-08

About Security Update 2006-001

web.archive.org  
text/html  
Inactive Link Not Archived

CONFIRM  
docs.info.apple.com/article.html?artnum=303382

Secunia - Advisories - Mandriva update for php

web.archive.org  
text/html

SECUNIA 17557

No Description Provided

www.osvdb.org  
Inactive Link Not Archived

OSVDB 20491

US-CERT Technical Cyber Security Alert TA06-062A -- Apple Mac Products are Affected by Multiple Vulnerabilities

US Government Resource  
www.us-cert.gov  
text/html

CERT TA06-062A

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](mailto: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     | 4.0.0   | 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     | 4.0.5   | 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 | 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 | 5.0.1  | 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 | 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 | 4.0.5  | 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 | 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 | 5.0.1 | 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 |
| 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:4.0.5:*****:        |     |     |       |     |     |     |
| 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: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:5.0.1:*****:     |
| 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:5.0.4:\*:\*:\*:\*:\*:\*:

cpe:2.3:a:php:php:5.0.5:\*:\*:\*:\*:\*:\*:

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:4.0.5:\*:\*:\*:\*:\*:

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: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:5.0.1:*****:   |
| 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:*****:   |

← Previous ID

Next ID→