

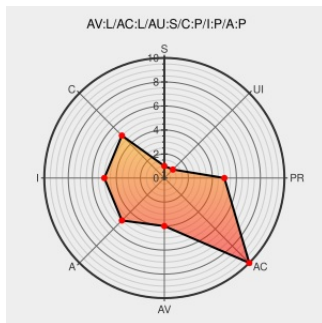


# CVE-2003-1307

Published on: 12/31/2003 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:44 PM UTC

## CVE-2003-1307

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

Certain versions of [Http Server](#) from [Apache](#) contain the following vulnerability:

**\*\* DISPUTED \*\*** The mod\_php module for the Apache HTTP Server allows local users with write access to PHP scripts to send signals to the server's process group and use the server's file descriptors, as demonstrated by sending a STOP signal, then intercepting incoming connections on the server's TCP port. NOTE: the PHP developer has disputed this vulnerability, saying "The opened file descriptors are opened by Apache. It is the job of Apache to protect them ... Not a bug in PHP."

CVE-2003-1307 has been assigned by [M](#) [cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access  
Vector

LOCAL

Access  
Complexity

LOW

Authentication

SINGLE

Confidentiality  
Impact

PARTIAL

Integrity  
Impact

PARTIAL

Availability  
Impact

PARTIAL

## CVE References

Description

Tags

Link

[www.securityfocus.com](http://www.securityfocus.com)  
[text/x-c](#)

[BUGTRAQ 20061020 Re: PHP "exec", "system", "popen" \(+small POC\)](#)

Apache mod\_php Module File Descriptor Leakage Vulnerability

[Exploit](#)  
[cve.report \(archive\)](#)  
[text/html](#)

[BUGTRAQ 20061020 Re: PHP "exec", "system", "popen" \(+small POC\)](#)

PHP Bugs: #38915: mod\_php: system() (and similar) don't cleanup opened handles of Apache

[Exploit](#)  
[bugs.php.net](#)  
[text/html](#)

[php](#) [MISC bugs.php.net/38915](http://MISC.bugs.php.net/38915)

Page not found - GitHub Pages

[Exploit](#)

[MISC hackerdom.ru/~dimmo/phpepl.c](#)

hackerdom.ru  
text/x-c  
Inactive Link Not Archived

SecurityFocus

www.securityfocus.com  
text/html

BUGTRAQ 20061019 PHP "exec",  
"system", "popen" problem

SecurityFocus HOME Mailing List: BugTraQ

Exploit  
Vendor Advisory  
www.securityfocus.com  
text/html

BUGTRAQ 20031226 Hijacking Apache  
https by mod\_php

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 | Apache | Http Server | 2.0     | All    | All     | All      |
| Application | Apache | Http Server | 2.0.28  | All    | All     | All      |
| Application | Apache | Http Server | 2.0.28  | beta   | All     | All      |
| Application | Apache | Http Server | 2.0.28  | beta   | win32   | All      |
| Application | Apache | Http Server | 2.0.32  | All    | All     | All      |
| Application | Apache | Http Server | 2.0.32  | beta   | win32   | All      |
| Application | Apache | Http Server | 2.0.34  | beta   | win32   | All      |
| Application | Apache | Http Server | 2.0.35  | All    | All     | All      |
| Application | Apache | Http Server | 2.0.36  | All    | All     | All      |
| Application | Apache | Http Server | 2.0.37  | All    | All     | All      |
| Application | Apache | Http Server | 2.0.38  | All    | All     | All      |
| Application | Apache | Http Server | 2.0.39  | All    | All     | All      |
| Application | Apache | Http Server | 2.0.40  | All    | All     | All      |
| Application | Apache | Http Server | 2.0.41  | All    | All     | All      |
| Application | Apache | Http Server | 2.0.42  | All    | All     | All      |
| Application | Apache | Http Server | 2.0.43  | All    | All     | All      |
| Application | Apache | Http Server | 2.0.44  | All    | All     | All      |
| Application | Apache | Http Server | 2.0.45  | All    | All     | All      |
| Application | Apache | Http Server | 2.0.46  | All    | All     | All      |
| Application | Apache | Http Server | 2.0.46  | All    | win32   | All      |
| Application | Apache | Http Server | 2.0.47  | All    | All     | All      |
| Application | Apache | Http Server | 2.0.48  | All    | All     | All      |

| Application                                             | Package | Component   | Version | Architecture | Operating System | Platform |
|---------------------------------------------------------|---------|-------------|---------|--------------|------------------|----------|
| Application                                             | Apache  | Http Server | 2.0.9   | All          | All              | All      |
| Application                                             | Apache  | Http Server | 2.0     | All          | All              | All      |
| Application                                             | Apache  | Http Server | 2.0.28  | All          | All              | All      |
| Application                                             | Apache  | Http Server | 2.0.28  | beta         | All              | All      |
| Application                                             | Apache  | Http Server | 2.0.28  | beta         | win32            | All      |
| Application                                             | Apache  | Http Server | 2.0.32  | All          | All              | All      |
| Application                                             | Apache  | Http Server | 2.0.32  | beta         | win32            | All      |
| Application                                             | Apache  | Http Server | 2.0.34  | beta         | win32            | All      |
| Application                                             | Apache  | Http Server | 2.0.35  | All          | All              | All      |
| Application                                             | Apache  | Http Server | 2.0.36  | All          | All              | All      |
| Application                                             | Apache  | Http Server | 2.0.37  | All          | All              | All      |
| Application                                             | Apache  | Http Server | 2.0.38  | All          | All              | All      |
| Application                                             | Apache  | Http Server | 2.0.39  | All          | All              | All      |
| Application                                             | Apache  | Http Server | 2.0.40  | All          | All              | All      |
| Application                                             | Apache  | Http Server | 2.0.41  | All          | All              | All      |
| Application                                             | Apache  | Http Server | 2.0.42  | All          | All              | All      |
| Application                                             | Apache  | Http Server | 2.0.43  | All          | All              | All      |
| Application                                             | Apache  | Http Server | 2.0.44  | All          | All              | All      |
| Application                                             | Apache  | Http Server | 2.0.45  | All          | All              | All      |
| Application                                             | Apache  | Http Server | 2.0.46  | All          | All              | All      |
| Application                                             | Apache  | Http Server | 2.0.46  | All          | win32            | All      |
| Application                                             | Apache  | Http Server | 2.0.47  | All          | All              | All      |
| Application                                             | Apache  | Http Server | 2.0.48  | All          | All              | All      |
| Application                                             | Apache  | Http Server | 2.0.9   | All          | All              | All      |
| cpe:2.3:a:apache:http_server:2.0:*:*:*:*:*:             |         |             |         |              |                  |          |
| cpe:2.3:a:apache:http_server:2.0.28:*:*:*:*:*:          |         |             |         |              |                  |          |
| cpe:2.3:a:apache:http_server:2.0.28:beta:*:*:*:*:       |         |             |         |              |                  |          |
| cpe:2.3:a:apache:http_server:2.0.28:beta:win32:*:*:*:*: |         |             |         |              |                  |          |
| cpe:2.3:a:apache:http_server:2.0.32:*:*:*:*:*:          |         |             |         |              |                  |          |
| cpe:2.3:a:apache:http_server:2.0.32:beta:win32:*:*:*:*: |         |             |         |              |                  |          |
| cpe:2.3:a:apache:http_server:2.0.34:beta:win32:*:*:*:*: |         |             |         |              |                  |          |
| cpe:2.3:a:apache:http_server:2.0.35:*:*:*:*:*:          |         |             |         |              |                  |          |
| cpe:2.3:a:apache:http_server:2.0.36:*:*:*:*:*:          |         |             |         |              |                  |          |

|                                                       |
|-------------------------------------------------------|
|                                                       |
| cpe:2.3:a:apache:http_server:2.0.37:*****:            |
| cpe:2.3:a:apache:http_server:2.0.38:*****:            |
| cpe:2.3:a:apache:http_server:2.0.39:*****:            |
| cpe:2.3:a:apache:http_server:2.0.40:*****:            |
| cpe:2.3:a:apache:http_server:2.0.41:*****:            |
| cpe:2.3:a:apache:http_server:2.0.42:*****:            |
| cpe:2.3:a:apache:http_server:2.0.43:*****:            |
| cpe:2.3:a:apache:http_server:2.0.44:*****:            |
| cpe:2.3:a:apache:http_server:2.0.45:*****:            |
| cpe:2.3:a:apache:http_server:2.0.46:*****:            |
| cpe:2.3:a:apache:http_server:2.0.46:*:win32:*****:    |
| cpe:2.3:a:apache:http_server:2.0.47:*****:            |
| cpe:2.3:a:apache:http_server:2.0.48:*****:            |
| cpe:2.3:a:apache:http_server:2.0.9:*****:             |
| cpe:2.3:a:apache:http_server:2.0:*****:               |
| cpe:2.3:a:apache:http_server:2.0.28:*****:            |
| cpe:2.3:a:apache:http_server:2.0.28:beta:*****:       |
| cpe:2.3:a:apache:http_server:2.0.28:beta:win32:*****: |
| cpe:2.3:a:apache:http_server:2.0.32:*****:            |
| cpe:2.3:a:apache:http_server:2.0.32:beta:win32:*****: |
| cpe:2.3:a:apache:http_server:2.0.34:beta:win32:*****: |
| cpe:2.3:a:apache:http_server:2.0.35:*****:            |
| cpe:2.3:a:apache:http_server:2.0.36:*****:            |
| cpe:2.3:a:apache:http_server:2.0.37:*****:            |
| cpe:2.3:a:apache:http_server:2.0.38:*****:            |
| cpe:2.3:a:apache:http_server:2.0.39:*****:            |
| cpe:2.3:a:apache:http_server:2.0.40:*****:            |
| cpe:2.3:a:apache:http_server:2.0.41:*****:            |
|                                                       |

|                                                    |
|----------------------------------------------------|
| cpe:2.3:a:apache:http_server:2.0.42:*****:         |
| cpe:2.3:a:apache:http_server:2.0.43:*****:         |
| cpe:2.3:a:apache:http_server:2.0.44:*****:         |
| cpe:2.3:a:apache:http_server:2.0.45:*****:         |
| cpe:2.3:a:apache:http_server:2.0.46:*****:         |
| cpe:2.3:a:apache:http_server:2.0.46:*:win32:*****: |
| cpe:2.3:a:apache:http_server:2.0.47:*****:         |
| cpe:2.3:a:apache:http_server:2.0.48:*****:         |
| cpe:2.3:a:apache:http_server:2.0.9:*****:          |

[← 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](#)