

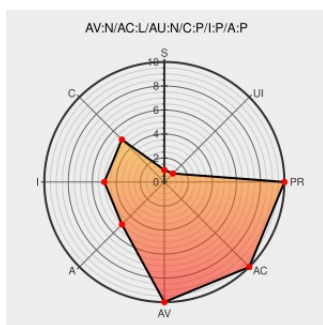


CVE-2005-3390

Published on: 10/31/2005 12:00:00 AM UTC

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

CVE-2005-3390

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

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

The RFC1867 file upload feature in PHP 4.x up to 4.4.0 and 5.x up to 5.0.5, when register_globals is enabled, allows remote attackers to modify the GLOBALS array and bypass security protections of PHP applications via a multipart/form-data POST request with a "GLOBALS" fileupload field.

CVE-2005-3390 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

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

[VUPEN ADV-2006-4320](#)

1. Overview:

[support.avaya.com](#)
[text/html](#)

[CONFIRM](#)
[support.avaya.com/elmodocs2/security/ASA-2006-037.htm](#)

SecurityTracker.com Archives - PHP Bug Lets Remote Users Overwrite the \$GLOBALS Array

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

[SECTrack 1015129](#)

Secunia - Advisories - SUSE update for php4/php5

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

[SECUNIA 18054](#)

Security Announcement

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

[SUSE SUSE-SR:2005:027](#)

[Inactive Link](#) [Not Archived](#)

IT Resource Center - login / register	web.archive.org text/html Inactive Link Not Archived	 HP SSRT061238
PHP File Upload GLOBAL Variable Overwrite Vulnerability	Patch cve.report (archive) text/html	 BID 15250
Advisories - Mandriva	www.mandriva.com text/html	 MANDRIVA MDKSA-2005:213
Hardened-PHP Project - PHP Security - GLOBALS Overwrite and it's consequences	www.hardened-php.net text/html	 MISC www.hardened-php.net/globals-problem
SecurityReason - PHP File-Upload \$GLOBALS Overwrite Vulnerability	securityreason.com text/html	 SREASON 132
OpenPKG: Security Advisory [OpenPKG-SA-2005.027-php]	www.openpkg.org text/html	 OPENPKG OpenPKG-SA-2005.027
rhn.redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2005:838
rhn.redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2005:831
Secunia - Advisories - Fedora update for php	web.archive.org text/html	 SECUNIA 17490
Red Hat Stronghold updates for uw-imap and PHP - Advisories - Secunia	web.archive.org text/html	 SECUNIA 21252
Hardened-PHP Project - PHP Security - Advisory 20/2005	Vendor Advisory www.hardened-php.net text/html	 MISC www.hardened-php.net/advisory_202005.79.html
HP System Management Homepage PHP Multiple Vulnerabilities - Advisories - Secunia	web.archive.org text/html	 SECUNIA 22691
usn.usn-232-1 - Ubuntu Linux	www.ubuntu.com text/html	 UBUNTU USN-232-1
Secunia - Advisories - SUSE Updates for Multiple Packages	web.archive.org text/html	 SECUNIA 17559
Secunia - Advisories - PHP Multiple Vulnerabilities	Patch Vendor Advisory web.archive.org text/html	 SECUNIA 17371
Secunia - Advisories - Gentoo update for php	web.archive.org text/html	 SECUNIA 17510
rhn.redhat.com Red Hat Support	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2006:0549
SecurityFocus	www.securityfocus.com text/html	 SUSE SUSE-SA:2005:069
The Fedora Legacy Project	web.archive.org text/html Inactive Link Not Archived	 FEDORA FLSA:166943
Secunia - Advisories - Avaya Products PHP Multiple Vulnerabilities	web.archive.org text/html	 SECUNIA 18669
PHP: PHP 4.4.1 Release Announcement	Patch	 CONFIRM www.php.net/release_4_4_1.php

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

Secunia - Advisories - Red Hat update for php

web.archive.org[text/html](#) SECUNIA 17531

SecurityFocus

www.securityfocus.com[text/html](#) BUGTRAQ 20051031 Advisory 20/2005: PHP File-Upload \$GLOBALS Overwrite Vulnerability

Repository / Oval Repository

oval.cisecurity.org[text/html](#) OVAL oval:org.mitre.oval:def:10537

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

Secunia - Advisories - Mandriva update for php

web.archive.org[text/html](#) SECUNIA 17557

Webmail - OVH

www.vupen.com[text/html](#) VUPEN ADV-2005-2254

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	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

Platform	Framework	Language	Version	Architecture	Deployment	License
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	4.0.0	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	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	4.0.0	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: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:4.0.0:*:*:*:*:*:						
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:*:*:*:*:*:
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:4.0.0:*****:
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:*****:

No vendor comments have been submitted for this CVE

[← 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](#)