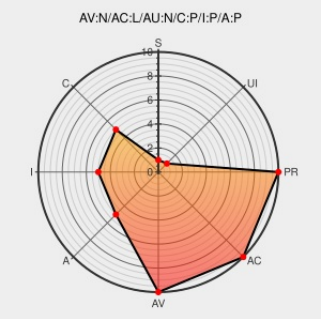
CVE-2007-3997

Published on: 09/04/2007 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:33 PM UTC

CVE-2007-3997

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Php from Php contain the following vulnerability:

The (1) MySQL and (2) MySQLi extensions in PHP 4 before 4.4.8, and PHP 5 before 5.2.4, allow remote attackers to bypass safe_mode and open_basedir restrictions via MySQL LOCAL INFILE operations, as demonstrated by a query with LOAD DATA LOCAL INFILE.

CVE-2007-3997 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Permissions Required, Third Party Advisory, www.vupen.com, text/html	VUPEN ADV-2007-3023
	Broken Link, www.trustix.org, text/plain, Inactive Link, Not Archived	TRUSTIX 2007-0026
PHP: PHP 4 ChangeLog	Vendor Advisory, www.php.net, text/html	CONFIRM www.php.net/ChangeLog-4.php
rPath Update for Multiple php Packages - Advisories - Secunia	Third Party Advisory, web.archive.org, text/html	SECUNIA 26838

PHP: PHP 5.2.4 Release Announcement	Vendor Advisory www.php.net text/html	CONFIRM www.php.net/releases/5_2_4.php
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Permissions Required Third Party Advisory www.vupen.com text/html	VUPEN ADV-2008-0059
PHP Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	Third Party Advisory web.archive.org text/html	SECUNIA 28318
No Description Provided	Broken Link issues.rpath.com Inactive Link Not Archived	CONFIRM issues.rpath.com/browse/RPL-1702
Gentoo Linux Documentation -- PHP: Multiple vulnerabilities	Third Party Advisory www.gentoo.org text/html	GENTOO GLSA-200710-02
No Description Provided	Broken Link issues.rpath.com Inactive Link Not Archived	CONFIRM issues.rpath.com/browse/RPL-1693
PHP MySQL/MySQLi Safe Mode Bypass Vulnerability	Exploit Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MISC secweb.se/en/advisories/php-mysql-safe-mode-bypass-vulnerability/
Gentoo update for php - Advisories - Secunia	Third Party Advisory web.archive.org text/html	SECUNIA 27102
IBM X-Force Exchange	Third Party Advisory VDB Entry exchange.xforce.ibmcloud.com text/html	XF php-local-infile-security-bypass(36384)
rPath update for php, php-mysql and php-pgsql - Advisories - Secunia	Third Party Advisory web.archive.org text/html	SECUNIA 27377
PHP: PHP 5 ChangeLog	Vendor Advisory www.php.net text/html	CONFIRM www.php.net/ChangeLog-5.php#5.2.4
Trustix Update for Multiple Packages - Advisories - Secunia	Third Party Advisory web.archive.org text/html	SECUNIA 26822
PHP: PHP 4.4.8 Release Announcement	Vendor Advisory www.php.net text/html	CONFIRM www.php.net/releases/4_4_8.php
PHP <= 4.4.7 / 5.2.3 MySQL/MySQLi Safe Mode Bypass Vulnerability	Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 4392
IBM X-Force Exchange	Third Party Advisory VDB Entry	XF php-localinfile-mysql-security-bypass(39402)

	exchange.xforce.ibmcloud.com text/html	
SecurityReason - PHP MySQL/MySQLi Safe Mode Bypass Vulnerability	Exploit Third Party Advisory securityreason.com text/html	SREASON 3102
PHP Multiple Vulnerabilities - Advisories - Secunia	Third Party Advisory web.archive.org text/html	SECUNIA 26642

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	All	All	All	All
Application	Php	Php	All	All	All	All

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

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

← Previous ID

Next ID→