



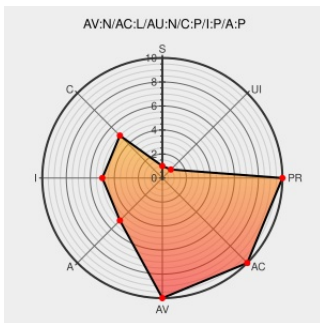
Last Modified on: 03/23/2021 11:25:20 PM UTC

CVE-2008-2107

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

Certain versions of `Php` from `Php` contain the following vulnerability:

The `GENERATE_SEED` macro in PHP 4.x before 4.4.8 and 5.x before 5.2.5, when running on 32-bit systems, performs a multiplication using values that can produce a zero seed in rare circumstances, which allows context-dependent attackers to predict subsequent values of the `rand` and `mt_rand` functions and possibly bypass protection mechanisms that rely on an unknown initial seed.

CVE-2008-2107 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
USN-628-1: PHP vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-628-1
Fedora update for php - Secunia Advisories - Vulnerability Intelligence - Secunia.com	web.archive.org text/html	 SECUNIA 30828
[SECURITY] Fedora 9 Update: php-5.2.6-2.fc9	www.redhat.com text/html	 FEDORA FEDORA-2008-3606
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval.org.mitre.oval:def:10644
Fedora update for php - Secunia Advisories - Vulnerability Intelligence - Secunia.com	web.archive.org text/html	 SECUNIA 30757
IBM X Force Exchange	exchange.xforce.ibmcloud.com	 XForce exchange.xforce.ibmcloud.com

IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF php-generateseed-security-bypass(42284)
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com	web.archive.org text/html	 SECUNIA 30967
rhnl.redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2008:0545
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF php-generateseed-weak-security(42226)
About Secunia Research Flexera	web.archive.org text/html	 SECUNIA 31200
Debian -- Security Information -- DSA-1789-1 php5	www.debian.org Deprecated Link text/html	 DEBIAN DSA-1789
Advisories Mandriva	www.mandriva.com text/html	 MANDRIVA MDVSA-2008:126
rhnl.redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2008:0582
404 Not Found	Exploit www.sektioneins.de text/plain Inactive Link Not Archived	 MISC www.sektioneins.de/advisories/SE-2008-02.txt
Advisories Mandriva	www.mandriva.com text/html	 MANDRIVA MDVSA-2008:127
SecurityFocus	www.securityfocus.com text/html	 BUGTRAQ 20080506 Advisory SE-2008-02: PHP GENERATE_SEED() Weak Random Number Seed Vulnerability
Advisories Mandriva	www.mandriva.com text/html	 MANDRIVA MDVSA-2008:125
No Description Provided	Exploit web.archive.org text/html Inactive Link Not Archived	 FULLDISC 20080506 Advisory SE-2008-02: PHP GENERATE_SEED() Weak Random Number Seed Vulnerability
Support / Security / Advisories // MDVSA-2008:129 Mandriva	www.mandriva.com text/html	 MANDRIVA MDVSA-2008:129
Red Hat update for php - Secunia Advisories - Vulnerability Intelligence - Secunia.com	web.archive.org text/html	 SECUNIA 31119
Support / Security / Advisories // MDVSA-2008:128 Mandriva	www.mandriva.com text/html	 MANDRIVA MDVSA-2008:128
Gentoo update for php - Secunia Advisories - Vulnerability Information - Secunia.com	web.archive.org text/html	 SECUNIA 32746
Red Hat update for php - Secunia Advisories - Vulnerability Intelligence - Secunia.com	web.archive.org text/html	 SECUNIA 31124
Support / Security / Advisories // MDVSA-2008:130 Mandriva	www.mandriva.com text/html	 MANDRIVA MDVSA-2008:130
Debian update for php5 - Secunia Advisories - Vulnerability Information - Secunia.com	web.archive.org text/html	 SECUNIA 35003
rhnl.redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2008:0546

[security-announce] SUSE Security Summary Report SUSE-SR:2008:014	lists.opensuse.org text/html	 SUSE SUSE-SR:2008:014
SecurityReason - PHP GENERATE_SEED() Weak Random Number Seed Vulnerability	securityreason.com text/html	 SREASON 3859
PHP: Multiple vulnerabilities — Gentoo Linux Documentation	security.gentoo.org text/html	 GENTOO GLSA-200811-05
rhn.redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2008:0544
[SECURITY] Fedora 8 Update: php-5.2.6-2.fc8	www.redhat.com text/html	 FEDORA FEDORA-2008-3864
rhn.redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2008:0505

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	5	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	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	5.1.3	All	All	All
Application	Php	Php	5.1.4	All	All	All
Application	Php	Php	5.1.5	All	All	All
Application	Php	Php	5.1.6	All	All	All

Application	Php	Php	5.1.0	All	All	All
Application	Php	Php	5.2.0	All	All	All
Application	Php	Php	5.2.1	All	All	All
Application	Php	Php	5.2.2	All	All	All
Application	Php	Php	5.2.3	All	All	All
Application	Php	Php	5.2.4	All	All	All
Application	Php	Php	5	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	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	5.1.3	All	All	All
Application	Php	Php	5.1.4	All	All	All
Application	Php	Php	5.1.5	All	All	All
Application	Php	Php	5.1.6	All	All	All
Application	Php	Php	5.2.0	All	All	All
Application	Php	Php	5.2.1	All	All	All
Application	Php	Php	5.2.2	All	All	All
Application	Php	Php	5.2.3	All	All	All
Application	Php	Php	5.2.4	All	All	All
Application	Php	Php	All	All	All	All
cpe:2.3:a:php:php:5.*.*.*.*.*.*.*.*						
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: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:*:*:*:*:*:
cpe:2.3:a:php:php:5.1.3:*:*:*:*:*:
cpe:2.3:a:php:php:5.1.4:*:*:*:*:*:
cpe:2.3:a:php:php:5.1.5:*:*:*:*:*:
cpe:2.3:a:php:php:5.1.6:*:*:*:*:*:
cpe:2.3:a:php:php:5.2.0:*:*:*:*:*:
cpe:2.3:a:php:php:5.2.1:*:*:*:*:*:
cpe:2.3:a:php:php:5.2.2:*:*:*:*:*:
cpe:2.3:a:php:php:5.2.3:*:*:*:*:*:
cpe:2.3:a:php:php:5.2.4:*:*:*:*:*:
cpe:2.3:a:php:php:5.*:*:*:*:*:
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: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:*****:
cpe:2.3:a:php:php:5.1.3:*****:
cpe:2.3:a:php:php:5.1.4:*****:
cpe:2.3:a:php:php:5.1.5:*****:
cpe:2.3:a:php:php:5.1.6:*****:
cpe:2.3:a:php:php:5.2.0:*****:
cpe:2.3:a:php:php:5.2.1:*****:
cpe:2.3:a:php:php:5.2.2:*****:
cpe:2.3:a:php:php:5.2.3:*****:
cpe:2.3:a:php:php:5.2.4:*****:
cpe:2.3:a:php:php:*****:

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](#)