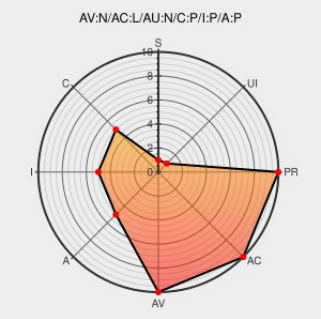
CVE-2008-2108

Published on: 05/07/2008 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:21 PM UTC

CVE-2008-2108

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 64-bit systems, performs a multiplication that generates a portion of zero bits during conversion due to insufficient precision, which produces 24 bits of entropy and simplifies brute force attacks against protection mechanisms that use the rand and mt_rand functions.

CVE-2008-2108 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
Fedora update for php - Secunia Advisories - Vulnerability Intelligence - Secunia.com	web.archive.org text/html	SECUNIA 30757
rhn.redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2008:0545
IBM X-Force Exchange	[illegible]	XF php-generatesseed-weak-security(42226)

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 Depreciated Link text/html	DEBIAN DSA-1789
Advisories | Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2008:126
rhn.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
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:10844
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
rhn.redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2008:0546
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

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	5.2.0	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→