



CVE-2010-1128

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2010-1128
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-03-26 20:30:00 UTC
Updated	2010-12-10 06:39:00 UTC
Description	The Linear Congruential Generator (LCG) in PHP before 5.2.13 does not provide the expected entropy, which makes it eas

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Php	Php	5.2.0	All	All	All
Application	Php	Php	5.2.1	All	All	All
Application	Php	Php	5.2.10	All	All	All
Application	Php	Php	5.2.11	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	5.2.5	All	All	All
Application	Php	Php	5.2.6	All	All	All
Application	Php	Php	5.2.7	All	All	All
Application	Php	Php	5.2.8	All	All	All
Application	Php	Php	5.2.9	All	All	All
Application	Php	Php	5.2.0	All	All	All
Application	Php	Php	5.2.1	All	All	All
Application	Php	Php	5.2.10	All	All	All
Application	Php	Php	5.2.11	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	5.2.5	All	All	All
Application	Php	Php	5.2.6	All	All	All
Application	Php	Php	5.2.7	All	All	All
Application	Php	Php	5.2.8	All	All	All
Application	Php	Php	5.2.9	All	All	All
Application	Php	Php	All	All	All	All

References			
Reference	Source	Link	Tags
Support	REDHAT	www.redhat.com	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com	
PHP LCG Entropy Security Vulnerability	BID	www.securityfocus.com	Exploit
PHP: PHP 5.2.13 Release Announcement	CONFIRM	www.php.net	Vendor Advisory
Red Hat update for php - Secunia.com	SECUNIA	secunia.com	
PHP Two Security Bypass Vulnerabilities - Advisories - Community	SECUNIA	secunia.com	Vendor Advisory
PHP: PHP 5 ChangeLog	CONFIRM	www.php.net	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com	Patch, Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit			
Organization	Published	Contributor	Statement
Red Hat	2010-04-14	Joshua Bressers	Red Hat is aware of this issue and is tracking it via the following bug: https://bugzilla.redhat.com/show_bug.cgi?id=52442

There are currently no legacy QID mappings associated with this CVE.