



CVE-2007-1375

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

Summary

CVE	CVE-2007-1375
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-03-10 00:19:00 UTC
Updated	2017-10-11 01:31:00 UTC
Description	Integer overflow in the substr_compare function in PHP 5.2.1 and earlier allows context-dependent attackers to read sensi

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Php	Php	All	All	All	All

References

Reference	Source	Link	Tags
Debian -- Security Information -- DSA-1283-1 php5	DEBIAN	www.debian.org	
PHP 5 Substr_Compare Integer Overflow Vulnerability	BID	www.securityfocus.com	
USN-455-1: PHP vulnerabilities Ubuntu	UBUNTU	www.ubuntu.com	
SUSE update for php - Advisories - Secunia	SECUNIA	secunia.com	
32780	OSVDB	www.osvdb.org	
Gentoo update for php - Advisories - Secunia	SECUNIA	secunia.com	
Ubuntu update for php - Advisories - Secunia	SECUNIA	secunia.com	
PHP: PHP 5.2.2 Release Announcement	CONFIRM	us2.php.net	
Gentoo Linux Documentation -- PHP: Multiple vulnerabilities	GENTOO	security.gentoo.org	
Debian update for php5 - Advisories - Secunia	SECUNIA	secunia.com	
PHP 5.2.1 - 'substr_compare()' Information Leak - Multiple local Exploit	EXPLOIT-DB	www.exploit-db.com	
Security Announcement	SUSE	www.novell.com	
MOPB-14-2007:PHP substr_compare() Information Leak Vulnerability	MISC	www.php-security.org	Exploit, Vendor Advisory

Mandriva update for php - Advisories - Secunia	SECUNIA	secunia.com	
Advisories Mandriva	MANDRIVA	www.mandriva.com	
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	2008-11-26	Mark J Cox	We do not consider this flaw to be a security issue as it is only exploitable by the script author. N
There are currently no legacy QID mappings associated with this CVE.			