



CVE-2007-1376

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2007-1376
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-03-10 00:19:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	The shmop functions in PHP before 4.4.5, and before 5.2.1 in the 5.x series, do not verify that their arguments correspond t

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:P/A:P

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Php	Php	4.0	All	All	All

Application	Php	Php	4.0	beta1	All	All
Application	Php	Php	4.0	beta2	All	All
Application	Php	Php	4.0	beta3	All	All
Application	Php	Php	4.0	beta4	All	All
Application	Php	Php	4.0	beta_4_patch1	All	All
Application	Php	Php	4.0	rc1	All	All
Application	Php	Php	4.0	rc2	All	All
Application	Php	Php	4.0.0	All	All	All
Application	Php	Php	4.0.1	All	All	All
Application	Php	Php	4.0.1	patch1	All	All
Application	Php	Php	4.0.1	patch2	All	All
Application	Php	Php	4.0.2	All	All	All
Application	Php	Php	4.0.3	All	All	All
Application	Php	Php	4.0.3	patch1	All	All
Application	Php	Php	4.0.4	All	All	All
Application	Php	Php	4.0.4	patch1	All	All
Application	Php	Php	4.0.5	All	All	All
Application	Php	Php	4.0.6	All	All	All
Application	Php	Php	4.0.7	All	All	All
Application	Php	Php	4.0.7	rc1	All	All
Application	Php	Php	4.0.7	rc2	All	All
Application	Php	Php	4.0.7	rc3	All	All
Application	Php	Php	4.1.0	All	All	All
Application	Php	Php	4.1.1	All	All	All
Application	Php	Php	4.1.2	All	All	All
Application	Php	Php	4.2	All	dev	All
Application	Php	Php	4.2.0	All	All	All
Application	Php	Php	4.2.1	All	All	All
Application	Php	Php	4.2.2	All	All	All
Application	Php	Php	4.2.3	All	All	All
Application	Php	Php	4.3.0	All	All	All
Application	Php	Php	4.3.1	All	All	All
Application	Php	Php	4.3.10	All	All	All
Application	Php	Php	4.3.11	All	All	All
Application	Php	Php	4.3.2	All	All	All
Application	Php	Php	4.3.3	All	All	All

Application	Php	Php	4.3.4	All	All	All
Application	Php	Php	4.3.5	All	All	All
Application	Php	Php	4.3.6	All	All	All
Application	Php	Php	4.3.7	All	All	All
Application	Php	Php	4.3.8	All	All	All
Application	Php	Php	4.3.9	All	All	All
Application	Php	Php	4.4.0	All	All	All
Application	Php	Php	4.4.1	All	All	All
Application	Php	Php	4.4.2	All	All	All
Application	Php	Php	4.4.3	All	All	All
Application	Php	Php	4.4.4	All	All	All
Application	Php	Php	4.4.5	All	All	All
Application	Php	Php	5.0	rc1	All	All
Application	Php	Php	5.0	rc2	All	All
Application	Php	Php	5.0	rc3	All	All
Application	Php	Php	5.0.0	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	beta4	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
Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References			
Reference	Source		L
SUSE update for php - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108		s
PHP < 4.4.5/5.2.1 - 'shmop' SSL RSA Private-Key Disclosure - Linux local Exploit	af854a3a-2127-422b-91ae-364da2661108		v
Security Announcement	af854a3a-2127-422b-91ae-364da2661108		v
PHP < 4.4.5/5.2.1 - 'shmop' Local Code Execution - Linux local Exploit	af854a3a-2127-422b-91ae-364da2661108		v
MOPB-15-2007:PHP shmop Functions Resource Verification Vulnerability	af854a3a-2127-422b-91ae-364da2661108		v
www.osvdb.org/32781	af854a3a-2127-422b-91ae-364da2661108		v
USN-455-1: PHP vulnerabilities Ubuntu	af854a3a-2127-422b-91ae-364da2661108		v
Gentoo update for php - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108		s
Debian update for php5 - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108		s
PHP Shared Memory Functions Resource Verification Arbitrary Code Execution Vulnerability	af854a3a-2127-422b-91ae-364da2661108		v
Gentoo Linux Documentation -- PHP: Multiple vulnerabilities	af854a3a-2127-422b-91ae-364da2661108		s
Ubuntu update for php - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108		s
Debian -- Security Information -- DSA-1283-1 php5	af854a3a-2127-422b-91ae-364da2661108		v
CVE Program record	CVE.ORG		v
NVD vulnerability detail	NVD		n

Vendor Comments And Credit			
Organization	Published	Contributor	Statement
Red Hat	2007-04-16	Mark J Cox	The PHP interpreter does not offer a reliable "sandboxed" security layer (as found in,

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

