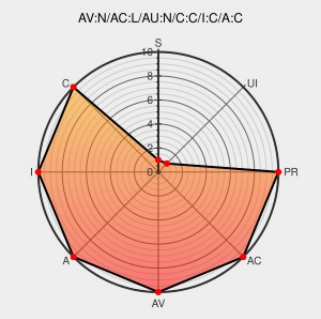
CVE-2004-1018

Published on: 12/08/2004 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:10 PM UTC

CVE-2004-1018

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

Multiple integer handling errors in PHP before 4.3.10 allow attackers to bypass safe mode restrictions, cause a denial of service, or execute arbitrary code via (1) a negative offset value to the shmop_write function, (2) an "integer overflow/underflow" in the pack function, or (3) an "integer overflow/underflow" in the unpack function. NOTE: this issue was originally REJECTed by its CNA before publication, but that decision is in active dispute. This candidate may change significantly in the future as a result of further discussion.

CVE-2004-1018 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
redhat.com | Red Hat Support	Third Party Advisory, www.redhat.com, text/html	REDHAT RHSA-2005:032
'Advisory 01/2004: Multiple vulnerabilities in PHP 4/5' - MARC	Issue Tracking, Third Party Advisory, marc.info, text/html	BUGTRAQ 20041215 Advisory 01/2004: Multiple vulnerabilities in PHP 4/5
Advisories - Mandriva	Third Party Advisory, www.mandriva.com, text/html	MANDRAKE MDKSA-2005:072

No Description Provided	Third Party Advisory VDB Entry web.archive.org text/html Inactive Link Not Archived	HP HPSBMA01212
IBM X-Force Exchange	Third Party Advisory VDB Entry exchange.xforce.ibmcloud.com text/html	XF php-shmopwrite-outofbounds-memory(18515)
Hardened PHP - Hardened-PHP	Third Party Advisory www.hardened-php.net text/plain	MISC www.hardened-php.net/advisories/012004.txt
Repository / Oval Repository	Third Party Advisory oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:10949
rhn.redhat.com | Red Hat Support	Third Party Advisory www.redhat.com text/html	REDHAT RHSA-2005:816
Advisories - Mandriva	Third Party Advisory www.mandriva.com text/html	MANDRAKE MDKSA-2004:151
usn/usn-99-1 - Ubuntu Linux	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-99-1
PHP: PHP 4.3.10 Release Announcement	Release Notes Vendor Advisory www.php.net text/html	CONFIRM www.php.net/release_4_3_10.php
No Description Provided	Broken Link bugzilla.fedora.us Inactive Link Not Archived	FEDORA FLSA:2344
SecurityFocus	Third Party Advisory VDB Entry www.securityfocus.com text/html	BUGTRAQ 20041219 PHP shmop.c module permits write of arbitrary memory.
PHP Shared Memory Module Offset Memory Corruption Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	BID 12045
No Description Provided	Broken Link www.osvdb.org Inactive Link Not Archived	OSVDB 12411

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	4.10	All	All	All
Operating System	Canonical	Ubuntu Linux	4.10	All	All	All
Application	Php	Php	All	All	All	All
Application	Php	Php	All	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:4.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:4.10:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:*:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→