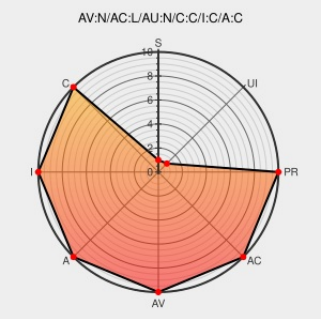
CVE-2004-1063

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

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

CVE-2004-1063

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



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

PHP 4.x to 4.3.9, and PHP 5.x to 5.0.2, when running in safe mode on a multithreaded Unix webserver, allows local users to bypass safe_mode_exec_dir restrictions and execute commands outside of the intended safe_mode_exec_dir via shell metacharacters in the current directory name. 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-2004-1063 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
Gentoo Linux Documentation -- PHP: Multiple vulnerabilities	Third Party Advisory, www.gentoo.org, text/html	GENTOO GLSA-200412-14
PHP Multiple Local And Remote Vulnerabilities	Third Party Advisory, VDB Entry, cve.report (archive), text/html	BID 11964
No Description Provided	Broken Link, www.osvdb.org	OSVDB 12412

	Inactive Link Not Archived	
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
SecurityFocus	Third Party Advisory VDB Entry www.securityfocus.com text/html	BUGTRAQ 20041215 Advisory 01/2004: Multiple vulnerabilities in PHP 4/5
Hardened PHP - Hardened-PHP	Third Party Advisory www.hardened-php.net text/plain	MISC www.hardened-php.net/advisories/012004.txt
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
IBM X-Force Exchange	Third Party Advisory VDB Entry exchange.xforce.ibmcloud.com text/html	XF php-safemodeexecdir-restriction-bypass(18511)
Home - Conectiva	Broken Link distro.conectiva.com.br text/html	CONECTIVA CLA-2005:915

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:*:*:*:*:*:*:*:*:

← Previous ID

Next ID→