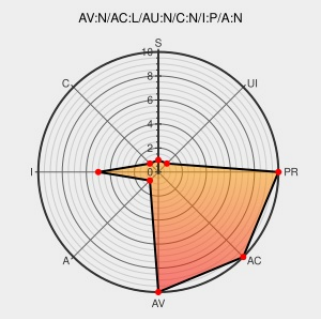
CVE-2005-3883

Published on: 11/29/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:23 PM UTC

CVE-2005-3883

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



Certain versions of Php from Php contain the following vulnerability:

CRLF injection vulnerability in the mb_send_mail function in PHP before 5.1.0 might allow remote attackers to inject arbitrary e-mail headers via line feeds (LF) in the "To" address argument.

CVE-2005-3883 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2006-2685
PHP MB_Send_Mail TO Argument Header Injection Vulnerability	Patch cve.report (archive) text/html	BID 15571
Secunia - Advisories - SUSE update for php4/php5	web.archive.org text/html	SECUNIA 18054
Secunia - Advisories - PHP "mb_send_mail()" "To:" Header Injection Vulnerability	Patch Vendor Advisory web.archive.org text/html	SECUNIA 17763
rhn.redhat.com | Red Hat Support	web.archive.org text/html	REDHAT RHSA-2006:0276

	Inactive Link Not Archived	
SecurityTracker.com Archives - PHP mb_send_mail() May Let Users Inject SMTP Headers	securitytracker.com text/html	SECTRACK 1015296
PHP: PHP 5.1.0 Release Announcement	Patch www.php.net text/html	CONFIRM www.php.net/release_5_1_0.php
usn/usn-232-1 - Ubuntu Linux	www.ubuntu.com text/html	UBUNTU USN-232-1
No Description Provided	patches.sgi.com Inactive Link Not Archived	SGI 20060501-01-U
SecurityFocus	www.securityfocus.com text/html	SUSE SUSE-SA:2005:069
ASA-2006-129 (RHSA-2006-0276)	support.avaya.com text/html	CONFIRM support.avaya.com/elmodocs2/security/ASA-2006-129.htm
Advisories - Mandriva	www.mandriva.com text/html	MANDRIVA MDKSA-2005:238
Secunia - Advisories - Avaya Products PHP Multiple Vulnerabilities	web.archive.org text/html	SECUNIA 20951
Red Hat update for php - Advisories - Secunia	web.archive.org text/html	SECUNIA 19832
404 Not Found	www.turbolinux.com text/plain Inactive Link Not Archived	TURBO TLSA-2006-38
Secunia - Advisories - Ubuntu update for php4/php5	web.archive.org text/html	SECUNIA 18198
PHP Bugs: #35307: [PATCH] header can be injected when using mb_send_mail()	bugs.php.net text/html	MISC bugs.php.net/bug.php?id=35307
Secunia - Advisories - SGI Advanced Linux Environment Multiple Updates	web.archive.org text/html	SECUNIA 20210
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:10332
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF php-mbsendmail-header-injection(23270)

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	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	5.0.1	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	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	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	5.0.1	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

cpe:2.3:a:php:php:4.0.6:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.0.7:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.0.7:rc1:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.0.7:rc2:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.0.7:rc3:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.2:*:dev:*:*:*:*:*:

cpe:2.3:a:php:php:4.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.3.10:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.3.11:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.3.3:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.3.4:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.3.5:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.3.6:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.3.7:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.3.8:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.3.9:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0:rc3:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.1:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.2:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.3:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.4:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.5:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.0.6:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.0.7:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.0.7:rc1:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.0.7:rc2:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.0.7:rc3:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.1.0:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.1.1:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.1.2:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.2:*:dev:*:*:*:*:

cpe:2.3:a:php:php:4.2.0:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.2.1:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.2.2:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.2.3:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.3.0:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.3.1:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.3.10:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.3.11:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.3.2:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.3.3:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.3.4:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.3.5:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.3.6:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.3.7:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.3.8:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.3.9:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0:rc3:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.5:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→