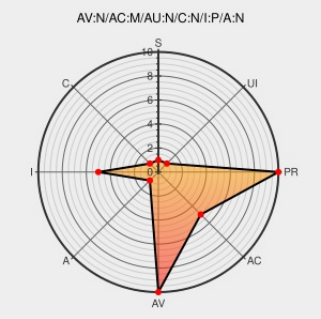
CVE-2005-3388

Published on: 10/31/2005 12:00:00 AM UTC

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

CVE-2005-3388

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



Certain versions of Php from Php contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in the phpinfo function in PHP 4.x up to 4.4.0 and 5.x up to 5.0.5 allows remote attackers to inject arbitrary web script or HTML via a crafted URL with a "stacked array assignment."

CVE-2005-3388 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	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-2006-4320
1. Overview:	support.avaya.com text/html	CONFIRM support.avaya.com/elmodocs2/security/ASA-2006-037.htm
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20051031 Advisory 18/2005: PHP Cross Site Scripting (XSS) Vulnerability in phpinfo()
Hardened-PHP Project - PHP Security - Advisory 18/2005	Vendor Advisory www.hardened-php.net text/html	MISC www.hardened-php.net/advisory_182005.77.html
Security Announcement	web.archive.org text/html	SUSE SUSE-SR:2005:027

	Inactive Link Not Archived	
SecurityTracker.com Archives - PHP Input Validation Hole in phpinfo() in Processing Stacked Array Contents Lets Remote Users Conduct Cross-Site Scripting Attacks	securitytracker.com text/html	SECTRACK 1015130
IT Resource Center - login / register	web.archive.org text/html Inactive Link Not Archived	HP SSRT061238
Advisories - Mandriva	www.mandriva.com text/html	MANDRIVA MDKSA-2005:213
OpenPKG: Security Advisory [OpenPKG-SA-2005.027-php]	www.openpkg.org text/html	OPENPKG OpenPKG-SA-2005.027
rhn.redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2005:838
rhn.redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2005:831
Secunia - Advisories - Fedora update for php	web.archive.org text/html	SECUNIA 17490
PHP PHPInfo Cross-Site Scripting Vulnerability	Patch cve.report (archive) text/html	BID 15248
Red Hat Stronghold updates for uw-imap and PHP - Advisories - Secunia	web.archive.org text/html	SECUNIA 21252
HP System Management Homepage PHP Multiple Vulnerabilities - Advisories - Secunia	web.archive.org text/html	SECUNIA 22691
usn/usn-232-1 - Ubuntu Linux	www.ubuntu.com text/html	UBUNTU USN-232-1
Secunia - Advisories - SUSE Updates for Multiple Packages	web.archive.org text/html	SECUNIA 17559
Secunia - Advisories - PHP Multiple Vulnerabilities	Patch Vendor Advisory web.archive.org text/html	SECUNIA 17371
Secunia - Advisories - Gentoo update for php	web.archive.org text/html	SECUNIA 17510
rhn.redhat.com | Red Hat Support	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2006:0549
The Fedora Legacy Project	web.archive.org text/html Inactive Link Not Archived	FEDORA FLSA:166943
Secunia - Advisories - Avaya Products PHP Multiple Vulnerabilities	web.archive.org text/html	SECUNIA 18669
PHP: PHP 4.4.1 Release Announcement	Patch www.php.net text/html	CONFIRM www.php.net/release_4_4_1.php
Secunia - Advisories - Red Hat update for php	web.archive.org text/html	SECUNIA 17531
404 Not Found	www.turbolinux.com	TURBO TLSA-2006-38

	text/plain Inactive Link Not Archived	
Secunia - Advisories - Ubuntu update for php4/php5	web.archive.org text/html	SECUNIA 18198
Gentoo Linux Documentation -- PHP: Multiple vulnerabilities	www.gentoo.org text/html	GENTOO GLSA-200511-08
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:10542
[SECURITY] Fedora 32 Update: ca-certificates-2020.2.41-1.1.fc32 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2020-fb144e7de5
Secunia - Advisories - Mandriva update for php	web.archive.org text/html	SECUNIA 17557
Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2005-2254
PHP Cross Site Scripting (XSS) Vulnerability in phpinfo() - CXSecurity.com	securityreason.com text/html	SREASON 133

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	4.0.0	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	4.0.5	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	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	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	4.0.5	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	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

cpe:2.3:a:php:php:4.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.0.1:patch1:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.0.1:patch2:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.0.3:patch1:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.0.5:*:*:*:*:*:*:*:

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:4.2.2:*:*:*:*:*:*:*:

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:5.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:beta1:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:beta2:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:beta3:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:beta4:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:rc3:*:*:*:*:*:*:

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:4.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.0.1:patch1:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.0.1:patch2:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.0.3:patch1:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.0.5:*:*:*:*:*:*:*:

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:4.3.5:*:*:*:*:*:*:*:

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:5.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:beta1:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:beta2:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:beta3:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:beta4:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.0.0:rc3:*:*:*:*:*:*:

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→