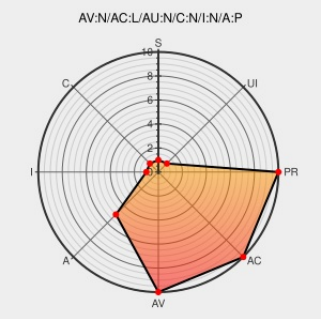
CVE-2005-3353

Published on: 11/18/2005 12:00:00 AM UTC

Last Modified on: 02/13/2023 02:10:42 AM UTC

CVE-2005-3353

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



Certain versions of Php from Php contain the following vulnerability:

The exif_read_data function in the Exif module in PHP before 4.4.1 allows remote attackers to cause a denial of service (infinite loop) via a malformed JPEG image.

CVE-2005-3353 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2006-4320
Mac OS X Security Update Fixes Multiple Vulnerabilities - Advisories - Secunia	web.archive.org text/html	SECUNIA 19064
Secunia - Advisories - SUSE update for php4/php5	web.archive.org text/html	SECUNIA 18054
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2006-0791
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF php-exif-dos(24351)
SecurityReason	securityreason.com text/html	SREASON 525

IT Resource Center - login / register	web.archive.org text/html Inactive Link Not Archived	HP SSRT061238
PHP Bugs: #34704: Infinite recursion due to corrupt JPEG	Exploit Patch Vendor Advisory bugs.php.net text/html	MISC bugs.php.net/bug.php?id=34704
Advisories - Mandriva	www.mandriva.com text/html	MANDRIVA MDKSA-2005:213
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:11032
PHP: PHP 4 ChangeLog	www.php.net text/html	CONFIRM www.php.net/ChangeLog-4.php#4.4.1
OpenPKG: Security Advisory [OpenPKG-SA-2005.027-php]	www.openpkg.org text/html	OPENPKG OpenPKG-SA-2005.027
Debian update for php4 - Advisories - Secunia	web.archive.org text/html	SECUNIA 22713
Secunia - Advisories - Fedora update for php	web.archive.org text/html	SECUNIA 17490
APPLE-SA-2006-03-01 Security Update 2006-001	lists.apple.com text/html	APPLE APPLE-SA-2006-03-01
HP System Management Homepage PHP Multiple Vulnerabilities - Advisories - Secunia	web.archive.org text/html	SECUNIA 22691
Apple Mac OS X Security Update 2006-001 Multiple Vulnerabilities	cve.report (archive) text/html	BID 16907
usn/usn-232-1 - Ubuntu Linux	www.ubuntu.com text/html	UBUNTU USN-232-1
Secunia - Advisories - PHP Multiple Vulnerabilities	web.archive.org text/html	SECUNIA 17371
SecurityFocus	www.securityfocus.com text/html	SUSE SUSE-SA:2005:069
The Fedora Legacy Project	web.archive.org text/html Inactive Link Not Archived	FEDORA FLSA:166943
Debian -- Security Information -- DSA-1206-1 php4	www.debian.org Depreciated Link text/html	DEBIAN DSA-1206
rhn.redhat.com | Red Hat Support	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2005:831
Secunia - Advisories - Red Hat update for php	web.archive.org text/html	SECUNIA 17531
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
About Security Update 2006-001	web.archive.org text/html Inactive Link Not Archived	CONFIRM docs.info.apple.com/article.html?artnum=303382
Secunia - Advisories - Mandriva update for php	web.archive.org text/html	SECUNIA 17557
US-CERT Technical Cyber Security Alert TA06-062A -- Apple Mac Products are Affected by Multiple Vulnerabilities	US Government Resource www.us-cert.gov text/html	CERT TA06-062A
PHP Group Exif Module Infinite Recursion Denial Of Service Vulnerability	cve.report (archive) text/html	BID 15358

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	4.0.2	All	All	All
Application	Php	Php	4.0.3	All	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	4.1.0	All	All	All
Application	Php	Php	4.1.1	All	All	All
Application	Php	Php	4.1.2	All	All	All
Application	Php	Php	4.2.0	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	4.0.0	All	All	All
Application	Php	Php	4.0.1	All	All	All
Application	Php	Php	4.0.2	All	All	All
Application	Php	Php	4.0.3	All	All	All
Application	Php	Php	4.0.4	All	All	All
Application	Php	Php	4.0.5	All	All	All
Application	Php	Php	4.0.6	All	All	All
Application	Php	Php	4.1.0	All	All	All
Application	Php	Php	4.1.1	All	All	All
Application	Php	Php	4.1.2	All	All	All
Application	Php	Php	4.2.0	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

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

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

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

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

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:4.1.0:*:*:*:*:*:*:*:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report