CVE-2008-3658

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2008-3658
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-08-15 00:41:00 UTC
Updated	2018-10-11 20:49:00 UTC
Description	Buffer overflow in the imageloadfont function in ext/gd/gd.c in PHP 4.4.x before 4.4.9 and PHP 5.2 before 5.2.6-r6 allows cc

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Php	Php	4.4.0	All	All	All
Application	Php	Php	4.4.1	All	All	All
Application	Php	Php	4.4.2	All	All	All
Application	Php	Php	4.4.3	All	All	All
Application	Php	Php	4.4.4	All	All	All
Application	Php	Php	4.4.5	All	All	All
Application	Php	Php	4.4.6	All	All	All
Application	Php	Php	4.4.7	All	All	All
Application	Php	Php	4.4.8	All	All	All
Application	Php	Php	5.2.0	All	All	All
Application	Php	Php	5.2.1	All	All	All
Application	Php	Php	5.2.2	All	All	All
Application	Php	Php	5.2.3	All	All	All
Application	Php	Php	5.2.4	All	All	All
Application	Php	Php	5.2.5	All	All	All
Application	Php	Php	5.2.6	All	All	All
Application	Php	Php	4.4.0	All	All	All

Application	Php	Php	4.4.1	All	All	All
Application	Php	Php	4.4.2	All	All	All
Application	Php	Php	4.4.3	All	All	All
Application	Php	Php	4.4.4	All	All	All
Application	Php	Php	4.4.5	All	All	All
Application	Php	Php	4.4.6	All	All	All
Application	Php	Php	4.4.7	All	All	All
Application	Php	Php	4.4.8	All	All	All
Application	Php	Php	5.2.0	All	All	All
Application	Php	Php	5.2.1	All	All	All
Application	Php	Php	5.2.2	All	All	All
Application	Php	Php	5.2.3	All	All	All
Application	Php	Php	5.2.4	All	All	All
Application	Php	Php	5.2.5	All	All	All
Application	Php	Php	5.2.6	All	All	All

References

Reference	Source
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
IBM X-Force Exchange	XF
'[security bulletin] HPSBUX02465 SSRT090192 rev.1 - HP-UX Running Apache-based Web Server, Remote Den' - MARC	HP
Fedora update for php - Advisories - Community	SECUNIA
oss-security - CVE request: php-5.2.6 overflow issues	MLIST
[security-announce] SUSE Security Summary Report: SUSE-SR:2008:018	SUSE
[security-announce] SUSE Security Summary Report: SUSE-SR:2008:021	SUSE
Repository / Oval Repository	OVAL
SecurityFocus	BUGTRAC
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
PHP: News Archive - 2008	CONFIRM
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
HP-UX update for Apache - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
Gentoo Bug 234102 - dev-lang/php < 5.2.6-r6: arbitrary code execution, DoS, safe_mode bypass (CVE-2008-{3658,3659,3660})	CONFIRM
Support / Security / Advisories / / MDVSA-2009:024 | Mandriva	MANDRIV
PHP Multiple Buffer Overflow Vulnerabilities	BID
Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA

About Secunia Research | Flexera	SECUNIA
php.cvs: cvs: php-src(PHP_5_2) /ext/gd gd.c /ext/gd/tests imageloadfont_invalid.phpt	MISC
About the security content of Security Update 2009-002 / Mac OS X v10.5.7	CONFIRM
US-CERT Technical Cyber Security Alert TA09-133A -- Apple Updates for Multiple Vulnerabilities	CERT
[SECURITY] Fedora 9 Update: maniadrive-1.2-13.fc9	FEDORA
Debian -- Security Information -- DSA-1647-1 php5	DEBIAN
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Gentoo update for php - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
47484	OSVDB
rhn.redhat.com | Red Hat Support	REDHAT
Advisories | Mandriva	MANDRIV
Advisories | Mandriva	MANDRIV
Advisories:rPSA-2009-0035 - rPath Wiki	CONFIRM
APPLE-SA-2009-05-12 Security Update 2009-002 / Mac OS X v10.5.7	APPLE
Advisories | Mandriva	MANDRIV
oss-security - Re: CVE request: php-5.2.6 overflow issues	MLIST
[SECURITY] Fedora 10 Update: maniadrive-1.2-13.fc10	FEDORA
SecurityFocus	HP
HPSBUX02401	HP
PHP: Multiple vulnerabilities — Gentoo Linux Documentation	GENTOO
HP Secure Web Server/Internet Express for Tru64 UNIX PHP Vulnerability - Secunia.com	SECUNIA
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2009-04-07	Joshua Bressers	This issue has been addressed in the affected versions of PHP packages shipped in Red Ha

There are currently no legacy QID mappings associated with this CVE.

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

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