



CVE-2010-4698

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2010-4698
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-01-18 20:00:00 UTC
Updated	2017-09-19 01:31:00 UTC
Description	Stack-based buffer overflow in the GD extension in PHP before 5.2.15 and 5.3.x before 5.3.4 allows context-dependent att

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Php	Php	5.2.0	All	All	All
Application	Php	Php	5.2.1	All	All	All
Application	Php	Php	5.2.10	All	All	All
Application	Php	Php	5.2.11	All	All	All
Application	Php	Php	5.2.12	All	All	All
Application	Php	Php	5.2.13	All	All	All
Application	Php	Php	5.2.14	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	5.3.0	All	All	All
Application	Php	Php	5.3.1	All	All	All
Application	Php	Php	5.3.2	All	All	All
Application	Php	Php	5.3.3	All	All	All
Application	Php	Php	5.2.0	All	All	All
Application	Php	Php	5.2.1	All	All	All
Application	Php	Php	5.2.10	All	All	All

Application	Php	Php	5.2.11	All	All	All
Application	Php	Php	5.2.12	All	All	All
Application	Php	Php	5.2.13	All	All	All
Application	Php	Php	5.2.14	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	5.3.0	All	All	All
Application	Php	Php	5.3.1	All	All	All
Application	Php	Php	5.3.2	All	All	All
Application	Php	Php	5.3.3	All	All	All

References				
Reference	Source	Link		
PHP GD Extension 'imagepste' Function Stack Buffer Overflow Vulnerability	BID	www		
'[security bulletin] HPSBOV02763 SSRT100826 rev.1 - HP Secure Web Server (SWS) for OpenVMS running PH' - MARC	HP	mar		
PHP :: Bug #53492 :: Stack buffer overflow in imagepste	CONFIRM	bug		
Repository / Oval Repository	OVAL	ova		
Full Disclosure: PHP 5.3.3 GD extension imagepste stack buffer overflow	FULLDISC	sec		
PHP: PHP 5 ChangeLog	CONFIRM	ww		
CVE Program record	CVE.ORG	ww		
NVD vulnerability detail	NVD	nvd		

No vendor comments have been submitted for this CVE.

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