



CVE-2016-7398

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

Summary

CVE	CVE-2016-7398
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-09-06 19:15:00 UTC
Updated	2019-09-20 21:15:00 UTC
Description	A type confusion vulnerability in the merge_param() function of php_http_params.c in PHP's pecl-http extension 3.1.0beta2

Risk And Classification

Problem Types: CWE-704

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Php	Ext-http	2.6.0	-	All	All
Application	Php	Ext-http	2.6.0	beta1	All	All
Application	Php	Ext-http	2.6.0	beta2	All	All
Application	Php	Ext-http	2.6.0	rc1	All	All
Application	Php	Ext-http	3.1.0	All	All	All
Application	Php	Ext-http	3.1.0	beta1	All	All
Application	Php	Ext-http	3.1.0	beta2	All	All
Application	Php	Ext-http	3.1.0	rc1	All	All
Application	Php	Ext-http	2.6.0	-	All	All
Application	Php	Ext-http	2.6.0	beta1	All	All
Application	Php	Ext-http	2.6.0	beta2	All	All
Application	Php	Ext-http	2.6.0	rc1	All	All
Application	Php	Ext-http	3.1.0	All	All	All
Application	Php	Ext-http	3.1.0	beta1	All	All
Application	Php	Ext-http	3.1.0	beta2	All	All
Application	Php	Ext-http	3.1.0	rc1	All	All
Application	Php	Ext-http	All	All	All	All

Application	Php	Ext-http	All	All	All	All
References						
Reference	Source	Link	Tags			
PHP :: Sec Bug #73055 :: Type confusion vulnerability in merge_param()	MISC	bugs.php.net	Exploit, Mailing List, Vendor Adviso			
[SECURITY] [DLA 1929-1] php-pecl-http security update	MLIST	lists.debian.org				
fix bug #73055 · m6w6/ext-http@17137d4 · GitHub	MISC	github.com	Patch, Third Party Advisory			
PHP :: Sec Bug #73055 :: Type confusion vulnerability in merge_param()	MISC	bugs.php.net	Exploit, Vendor Advisory			
CVE Program record	CVE.ORG	www.cve.org	canonical			
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis			
No vendor comments have been submitted for this CVE.						
There are currently no legacy QID mappings associated with this CVE.						