CVE-2013-4352

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

Summary

CVE	CVE-2013-4352
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-07-20 11:12:00 UTC
Updated	2023-11-07 02:16:00 UTC
Description	The cache_invalidate function in modules/cache/cache_storage.c in the mod_cache module in the Apache HTTP Server 2.4

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	2.4.6	All	All	All
Application	Apache	Http Server	2.4.6	All	All	All

References

Reference	Source	Link	Tags
Pony Mail!		lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!		lists.apache.org	
Pony Mail!		lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
[Apache-SVN] Log of /httpd/httpd/trunk/modules/cache/cache_storage.c	CONFIRM	svn.apache.org	
Pony Mail!		lists.apache.org	
Pony Mail!		lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	

Pony Mail!		lists.apache.org	
Bug 1120604 – CVE-2013-4352 httpd: mod_cache NULL pointer dereference crash	CONFIRM	bugzilla.redhat.com	
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!		lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!		lists.apache.org	
[Apache-SVN] Diff of /httpd/httpd/trunk/modules/cache/cache_storage.c	CONFIRM	svn.apache.org	
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!		lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
Apache HTTP Server 2.4 vulnerabilities - The Apache HTTP Server Project	CONFIRM	httpd.apache.org	Vendor Advisory
Pony Mail!		lists.apache.org	
Pony Mail!		lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!		lists.apache.org	
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.