



CVE-2014-3523

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

Summary

CVE	CVE-2014-3523
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 02:20:00 UTC
Description	Memory leak in the winnt_accept function in server/mpm/winnt/child.c in the WinNT MPM in the Apache HTTP Server 2.4.x

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	2.4.1	All	All	All
Application	Apache	Http Server	2.4.2	All	All	All
Application	Apache	Http Server	2.4.3	All	All	All
Application	Apache	Http Server	2.4.4	All	All	All
Application	Apache	Http Server	2.4.6	All	All	All
Application	Apache	Http Server	2.4.7	All	All	All
Application	Apache	Http Server	2.4.8	All	All	All
Application	Apache	Http Server	2.4.9	All	All	All
Application	Apache	Http Server	2.4.1	All	All	All
Application	Apache	Http Server	2.4.2	All	All	All
Application	Apache	Http Server	2.4.3	All	All	All
Application	Apache	Http Server	2.4.4	All	All	All
Application	Apache	Http Server	2.4.6	All	All	All
Application	Apache	Http Server	2.4.7	All	All	All
Application	Apache	Http Server	2.4.8	All	All	All
Application	Apache	Http Server	2.4.9	All	All	All
Operating System	Microsoft	Windows	All	All	All	All

Operating System	Microsoft	Windows	All	All	All	All	
References							
Reference						Source	Link
Pony Mail!							listserv
Pony Mail!							listserv
Pony Mail!						MLIST	listserv
Pony Mail!						MLIST	listserv
Pony Mail!						MLIST	listserv
Pony Mail!							listserv
Pony Mail!							listserv
Pony Mail!							listserv
Pony Mail!						MLIST	listserv
Pony Mail!							listserv
[Apache-SVN] Log of /httpd/httpd/trunk/server/mpm/winnt/child.c						CONFIRM	svn
'[security bulletin] HPSBMU03409 rev.1 - HP Matrix Operating Environment, Multiple Vulnerabilities' - MARC						HP	marc
Pony Mail!							listserv
Pony Mail!						MLIST	listserv
Pony Mail!						MLIST	listserv
Pony Mail!							listserv
Pony Mail!							listserv
Pony Mail!						MLIST	listserv
Pony Mail!						MLIST	listserv
Pony Mail!						MLIST	listserv
Pony Mail!							listserv
Pony Mail!						MLIST	listserv
Apache HTTP Server CVE-2014-3523 Remote Denial of Service Vulnerability						BID	www
Pony Mail!						MLIST	listserv
'[security bulletin] HPSBMU03380 rev.1 - HP System Management Homepage (SMH) on Linux and Windows, Mu' - MARC						HP	marc
Pony Mail!							listserv
Pony Mail!						MLIST	listserv
Pony Mail!							listserv
[Apache-SVN] Diff of /httpd/httpd/trunk/server/mpm/winnt/child.c						CONFIRM	svn
Red Hat Customer Portal						REDHAT	rhn
Pony Mail!						MLIST	listserv
Apache HTTP Server CVE-2014-3523 Remote Denial of Service Vulnerability						CONFIRM	www

Apache HTTP Server 2.4 vulnerabilities - The Apache HTTP Server Project	CONFIRM	http
Pony Mail!		lists
Pony Mail!	MLIST	lists
Pony Mail!		lists
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvc



No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered 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](#)