



CVE-2004-0940

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2004-0940
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-02-09 05:00:00 UTC
Updated	2024-02-02 03:05:00 UTC
Description	Buffer overflow in the get_tag function in mod_include for Apache 1.3.x to 1.3.32 allows local users who can create SSI doc

Risk And Classification

Problem Types: CWE-131

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	1.3	All	All	All
Application	Apache	Http Server	1.3.1	All	All	All
Application	Apache	Http Server	1.3.11	All	All	All
Application	Apache	Http Server	1.3.12	All	All	All
Application	Apache	Http Server	1.3.14	All	All	All
Application	Apache	Http Server	1.3.17	All	All	All
Application	Apache	Http Server	1.3.18	All	All	All
Application	Apache	Http Server	1.3.19	All	All	All
Application	Apache	Http Server	1.3.20	All	All	All
Application	Apache	Http Server	1.3.22	All	All	All
Application	Apache	Http Server	1.3.23	All	All	All
Application	Apache	Http Server	1.3.24	All	All	All
Application	Apache	Http Server	1.3.25	All	All	All
Application	Apache	Http Server	1.3.26	All	All	All
Application	Apache	Http Server	1.3.27	All	All	All
Application	Apache	Http Server	1.3.28	All	All	All
Application	Apache	Http Server	1.3.29	All	All	All

Application	Apache	Http Server	1.3.3	All	All	All
Application	Apache	Http Server	1.3.31	All	All	All
Application	Apache	Http Server	1.3.32	All	All	All
Application	Apache	Http Server	1.3.4	All	All	All
Application	Apache	Http Server	1.3.6	All	All	All
Application	Apache	Http Server	1.3.7	All	dev	All
Application	Apache	Http Server	1.3.9	All	All	All
Application	Apache	Http Server	1.3	All	All	All
Application	Apache	Http Server	1.3.1	All	All	All
Application	Apache	Http Server	1.3.11	All	All	All
Application	Apache	Http Server	1.3.12	All	All	All
Application	Apache	Http Server	1.3.14	All	All	All
Application	Apache	Http Server	1.3.17	All	All	All
Application	Apache	Http Server	1.3.18	All	All	All
Application	Apache	Http Server	1.3.19	All	All	All
Application	Apache	Http Server	1.3.20	All	All	All
Application	Apache	Http Server	1.3.22	All	All	All
Application	Apache	Http Server	1.3.23	All	All	All
Application	Apache	Http Server	1.3.24	All	All	All
Application	Apache	Http Server	1.3.25	All	All	All
Application	Apache	Http Server	1.3.26	All	All	All
Application	Apache	Http Server	1.3.27	All	All	All
Application	Apache	Http Server	1.3.28	All	All	All
Application	Apache	Http Server	1.3.29	All	All	All
Application	Apache	Http Server	1.3.3	All	All	All
Application	Apache	Http Server	1.3.31	All	All	All
Application	Apache	Http Server	1.3.32	All	All	All
Application	Apache	Http Server	1.3.4	All	All	All
Application	Apache	Http Server	1.3.6	All	All	All
Application	Apache	Http Server	1.3.7	All	dev	All
Application	Apache	Http Server	1.3.9	All	All	All
Application	Apache	Http Server	All	All	All	All
Operating System	Hp	Hp-ux	11.00	All	All	All
Operating System	Hp	Hp-ux	11.11	All	All	All
Operating System	Hp	Hp-ux	11.20	All	All	All

Operating System	Hp	Hp-ux	11.22	All	All	All
Operating System	Hp	Hp-ux	11.00	All	All	All
Operating System	Hp	Hp-ux	11.11	All	All	All
Operating System	Hp	Hp-ux	11.20	All	All	All
Operating System	Hp	Hp-ux	11.22	All	All	All
Application	Openpkg	Openpkg	2.0	All	All	All
Application	Openpkg	Openpkg	2.1	All	All	All
Application	Openpkg	Openpkg	2.2	All	All	All
Application	Openpkg	Openpkg	current	All	All	All
Application	Openpkg	Openpkg	2.0	All	All	All
Application	Openpkg	Openpkg	2.1	All	All	All
Application	Openpkg	Openpkg	2.2	All	All	All
Application	Openpkg	Openpkg	current	All	All	All
Operating System	Slackware	Slackware Linux	10.0	All	All	All
Operating System	Slackware	Slackware Linux	8.0	All	All	All
Operating System	Slackware	Slackware Linux	8.1	All	All	All
Operating System	Slackware	Slackware Linux	9.0	All	All	All
Operating System	Slackware	Slackware Linux	9.1	All	All	All
Operating System	Slackware	Slackware Linux	current	All	All	All
Operating System	Slackware	Slackware Linux	10.0	All	All	All
Operating System	Slackware	Slackware Linux	8.0	All	All	All
Operating System	Slackware	Slackware Linux	8.1	All	All	All
Operating System	Slackware	Slackware Linux	9.0	All	All	All
Operating System	Slackware	Slackware Linux	9.1	All	All	All
Operating System	Slackware	Slackware Linux	current	All	All	All
Operating System	Suse	Suse Linux	8.0	All	All	All
Operating System	Suse	Suse Linux	8.1	All	All	All
Operating System	Suse	Suse Linux	8.2	All	All	All
Operating System	Suse	Suse Linux	9.0	All	All	All
Operating System	Suse	Suse Linux	9.0	All	x86_64	All
Operating System	Suse	Suse Linux	9.1	All	All	All
Operating System	Suse	Suse Linux	9.2	All	All	All
Operating System	Suse	Suse Linux	8.0	All	All	All
Operating System	Suse	Suse Linux	8.1	All	All	All
Operating System	Suse	Suse Linux	8.2	All	All	All

Operating System	Suse	Suse Linux	9.0	All	All	All
Operating System	Suse	Suse Linux	9.0	All	x86_64	All
Operating System	Suse	Suse Linux	9.1	All	All	All
Operating System	Suse	Suse Linux	9.2	All	All	All
Operating System	Trustix	Secure Linux	1.5	All	All	All
Operating System	Trustix	Secure Linux	1.5	All	All	All

References

Reference	Source	Link
Pony Mail!	MLIST	lists.apache.org
Pony Mail!		lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!		lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
Pony Mail!		lists.apache.org
1. Overview:	CONFIRM	support.avaya.com
Debian -- Security Information -- DSA-594-1 apache	DEBIAN	www.debian.org
Advisories - Mandriva	MANDRAKE	www.mandriva.com
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
Apache mod_include Local Buffer Overflow Vulnerability	BID	www.securityfocus.com/bid
httpd 1.3 vulnerabilities - The Apache HTTP Server Project	CONFIRM	www.apache.org
Secunia - Advisories - Sun Solaris Multiple Apache Vulnerabilities	SECUNIA	secunia.com
SecurityTracker.com Archives - Apache mod_include Buffer Overflow Lets Local Users Execute Arbitrary Code	SECTRACK	securitytracker.com
redhat.com Red Hat Support	REDHAT	www.redhat.com
Pony Mail!	MLIST	lists.apache.org
rhn.redhat.com Red Hat Support	REDHAT	www.redhat.com
Pony Mail!	MLIST	lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!		lists.apache.org
Secunia - Advisories - Apache "mod_include" Privilege Escalation Vulnerability	SECUNIA	secunia.com
Pony Mail!		lists.apache.org
Pony Mail!		lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!		lists.apache.org
#102197: Security Vulnerabilities in the Apache 1.3 Web Server	SUNALERT	sunsolve.sun.com

'[OpenPKG-SA-2004.047] OpenPKG Security Advisory (apache)' - MARC	OPENPKG	marc.info
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Apache	2008-07-02	Mark J Cox	Fixed in Apache HTTP Server 1.3.33: http://httpd.apache.org/security/vulnerabilities_13.html

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

© [CVE.report](http://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](http://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](http://mitre.org). This site includes MITRE data granted under the following [license](http://mitre.org).

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