



# CVE-2009-1955

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

## Summary

<b>CVE</b>	CVE-2009-1955
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2009-06-08 01:00:00 UTC
<b>Updated</b>	2024-02-02 14:11:00 UTC
<b>Description</b>	The expat XML parser in the apr_xml_* interface in xml/apr_xml.c in Apache APR-util before 1.3.7, as used in the mod_dav

## Risk And Classification

**Problem Types:** CWE-776

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Apache</a>	<a href="#">Apr-util</a>	All	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Apr-util</a>	All	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	All	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	All	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	All	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	6.06	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	8.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	8.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	9.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	6.06	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	8.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	8.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	9.04	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	10	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	11	All	All	All

Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	9	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	10	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	11	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	9	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Http Server</a>	-	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Http Server</a>	-	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Server</a>	9	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Server</a>	9	All	All	All

## References

Reference	Source
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
About Security Update 2009-006 / Mac OS X v10.6.2	CONFIR
oss-security - CVE request: "billion laughs" attack against Apache APR	MLIST
Oracle Critical Patch Update - April 2013	CONFIR
Pony Mail!	
Pony Mail!	MLIST
Pony Mail!	MLIST
Red Hat update for httpd - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNI
Pony Mail!	
IBM WebSphere Application Server Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNI
[SECURITY] Fedora 9 Update: apr-util-1.2.12-7.fc9	FEDORA
'[PATCH] prevent "billion laughs" attack against expat' - MARC	MLIST
Pony Mail!	
Apache APR-util Library Multiple Vulnerabilities - Advisories - Community	SECUNI
Pony Mail!	
Pony Mail!	
Pony Mail!	
Pony Mail!	MLIST
Apache mod_dav / svn Remote Denial of Service Exploit	EXPLOIT
Pony Mail!	
Apache APR-util Library Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNI
APPLE-SA-2009-11-09-1 Security Update 2009-006 / Mac OS X v10.6.2	APPLE
Pony Mail!	
Gentoo Linux Documentation -- APR Utility Library: Multiple vulnerabilities	GENTOO
Pony Mail!	MLIST

Pony Mail!	MLIS I
Ubuntu update for apache2 - Secunia.com	SECUNI
Pony Mail!	MLIST
Pony Mail!	MLIST
USN-787-1: Apache vulnerabilities   Ubuntu	UBUNTU
Pony Mail!	MLIST
Support / Security / Advisories // MDVSA-2009:131   Mandriva	MANDRI
IBM WebSphere Application Server for z/OS Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNI
Debian -- Security Information -- DSA-1812-1 apr-util	DEBIAN
Pony Mail!	
Apache APR-util 'xml/apr_xml.c' Denial of Service Vulnerability	BID
Pony Mail!	
[SECURITY] Fedora 10 Update: apr-util-1.3.7-1.fc10	FEDORA
SecurityFocus	BUGTRA
Support	REDHAT
Debian update for apr-util - Secunia.com	SECUNI
Slackware update for apr-util - Secunia.com	SECUNI
IBM Fix list for IBM WebSphere Application Server V7.0 - United States	CONFIR
USN-786-1: apr-util vulnerabilities   Ubuntu	UBUNTU
Pony Mail!	MLIST
Pony Mail!	
[security-announce] SUSE Security Summary Report: SUSE-SR:2010:011	SUSE
'[security bulletin] HPSBUX02612 SSRT100345 rev.1 - HP-UX Apache-based Web Server, Local Information' - MARC	HP
IBM PK99478: SHIP APAR FIXES FOR H28W700 FIX PACK 7.0.0.7. - United States	AIXAPAI
Support / Security / Advisories // MDVSA-2013:150   Mandriva	MANDRI
[Apache-SVN] Revision 781403	CONFIR
Pony Mail!	MLIST
Support	REDHAT
Pony Mail!	MLIST
Repository / Oval Repository	OVAL
Red Hat update for apr-util - Secunia.com	SECUNI
Gentoo update for apr-util - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNI
Pony Mail!	MLIST
PK91241: Z/OS IBM HTTP SERVER FOR WEBSHERE (POWERED BY APACHE) FIX PACK 6.1.0.27	AIXAPAI
Pony Mail!	
Pony Mail!	

[SECURITY] Fedora 11 Update: apr-util-1.3.7-1.fc11	FEDORA
IBM notice: The page you requested cannot be displayed	AIXAPAI
Fedora update for apr-util - Secunia.com	SECUNI
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
wiki.rpath.com/Advisories:rPSA-2009-0123	CONFIR
Pony Mail!	MLIST
The Slackware Linux Project: Slackware Security Advisories	SLACKV
Pony Mail!	MLIST
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
rPath update for apr-util - Secunia.com	SECUNI
Pony Mail!	MLIST
404 Not Found	CONFIR
Pony Mail!	
Repository / Oval Repository	OVAL
CVE Program record	CVE.OR
NVD vulnerability detail	NVD



No vendor comments have been submitted for this CVE.

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

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

**CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)**