



# CVE-2005-0699

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

## Summary

<b>CVE</b>	CVE-2005-0699
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2005-03-08 05:00:00 UTC
<b>Updated</b>	2017-10-11 01:29:00 UTC
<b>Description</b>	Multiple buffer overflows in the dissect_a11_radius function in the CDMA A11 (3G-A11) dissector (packet-3g-a11.c) for Eth

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Altlinux</a>	<a href="#">Alt Linux</a>	compact_2.3	All	All	All
Operating System	<a href="#">Altlinux</a>	<a href="#">Alt Linux</a>	junior_2.3	All	All	All
Operating System	<a href="#">Altlinux</a>	<a href="#">Alt Linux</a>	compact_2.3	All	All	All
Operating System	<a href="#">Altlinux</a>	<a href="#">Alt Linux</a>	junior_2.3	All	All	All
Operating System	<a href="#">Conectiva</a>	<a href="#">Linux</a>	10.0	All	All	All
Operating System	<a href="#">Conectiva</a>	<a href="#">Linux</a>	9.0	All	All	All
Operating System	<a href="#">Conectiva</a>	<a href="#">Linux</a>	10.0	All	All	All
Operating System	<a href="#">Conectiva</a>	<a href="#">Linux</a>	9.0	All	All	All
Application	<a href="#">Ethereal Group</a>	<a href="#">Ethereal</a>	0.10.3	All	All	All
Application	<a href="#">Ethereal Group</a>	<a href="#">Ethereal</a>	0.10.4	All	All	All
Application	<a href="#">Ethereal Group</a>	<a href="#">Ethereal</a>	0.10.5	All	All	All
Application	<a href="#">Ethereal Group</a>	<a href="#">Ethereal</a>	0.10.6	All	All	All
Application	<a href="#">Ethereal Group</a>	<a href="#">Ethereal</a>	0.10.7	All	All	All
Application	<a href="#">Ethereal Group</a>	<a href="#">Ethereal</a>	0.10.8	All	All	All
Application	<a href="#">Ethereal Group</a>	<a href="#">Ethereal</a>	0.10.9	All	All	All
Application	<a href="#">Ethereal Group</a>	<a href="#">Ethereal</a>	0.10.3	All	All	All
Application	<a href="#">Ethereal Group</a>	<a href="#">Ethereal</a>	0.10.4	All	All	All

Application	<a href="#">Ethereal Group</a>	<a href="#">Ethereal</a>	0.10.5	All	All	All
Application	<a href="#">Ethereal Group</a>	<a href="#">Ethereal</a>	0.10.6	All	All	All
Application	<a href="#">Ethereal Group</a>	<a href="#">Ethereal</a>	0.10.7	All	All	All
Application	<a href="#">Ethereal Group</a>	<a href="#">Ethereal</a>	0.10.8	All	All	All
Application	<a href="#">Ethereal Group</a>	<a href="#">Ethereal</a>	0.10.9	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	2.1	All	advanced_server	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	2.1	All	advanced_server_ia64	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	2.1	All	enterprise_server	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	2.1	All	enterprise_server_ia64	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	2.1	All	workstation	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	2.1	All	workstation_ia64	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	3.0	All	advanced_server	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	3.0	All	enterprise_server	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	3.0	All	workstation_server	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	4.0	All	advanced_server	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	4.0	All	enterprise_server	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	4.0	All	workstation	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	2.1	All	advanced_server	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	2.1	All	advanced_server_ia64	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	2.1	All	enterprise_server	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	2.1	All	enterprise_server_ia64	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	2.1	All	workstation	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	2.1	All	workstation_ia64	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	3.0	All	advanced_server	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	3.0	All	enterprise_server	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	3.0	All	workstation_server	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	4.0	All	advanced_server	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	4.0	All	enterprise_server	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	4.0	All	workstation	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	3.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	4.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	3.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	4.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux Advanced Workstation</a>	2.1	All	ia64	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux Advanced Workstation</a>	2.1	All	itanium_processor	All

Operating System	<a href="#">Redhat</a>	<a href="#">Linux Advanced Workstation</a>	2.1	All	ia64	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux Advanced Workstation</a>	2.1	All	itanium_processor	All

## References

Reference	Source	Link	Tags
SecurityFocus	BUGTRAQ	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	Exploit, Vendor Advisory
Ethereal RADIUS Authentication Dissection Buffer Overflow Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	Exploit, Patch, Vendor A
Ethereal: enpa-sa-00018	CONFIRM	<a href="http://www.ethereal.com">www.ethereal.com</a>	Exploit, Patch, Vendor A
Repository / Oval Repository	OVAL	<a href="http://oval.cisecurity.org">oval.cisecurity.org</a>	
Advisories - Mandriva	MANDRAKE	<a href="http://www.mandriva.com">www.mandriva.com</a>	
'Ethereal 0.10.9 and below remote root exploit' - MARC	BUGTRAQ	<a href="http://marc.info">marc.info</a>	
rhn.redhat.com   Red Hat Support	REDHAT	<a href="http://www.redhat.com">www.redhat.com</a>	Patch, Vendor Advisory
'RE: Ethereal remote buffer overflow - addon' - MARC	BUGTRAQ	<a href="http://marc.info">marc.info</a>	
[FLSA-2006:152922] Updated ethereal packages fix security issues	FEDORA	<a href="http://www.redhat.com">www.redhat.com</a>	
Gentoo Linux Documentation -- Ethereal: Multiple vulnerabilities	GENTOO	<a href="http://security.gentoo.org">security.gentoo.org</a>	Patch, Vendor Advisory
404 Not Found	MISC	<a href="http://security.lss.hr">security.lss.hr</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

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](#).

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