



# CVE-2007-1547

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2007-1547
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2007-03-20 22:19:00 UTC
<b>Updated</b>	2018-10-16 16:39:00 UTC
<b>Description</b>	The ReadRequestFromClient function in server/os/io.c in Network Audio System (NAS) before 1.8a SVN 237 allows remote

## 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="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	2007	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	2007	All	x86_64	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	2007	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	2007	All	x86_64	All
Application	<a href="#">Radscan</a>	<a href="#">Network Audio System</a>	1.8a	All	All	All
Application	<a href="#">Radscan</a>	<a href="#">Network Audio System</a>	1.8a	All	All	All

## References

Reference	Source	Link
Advisories - Mandriva Linux	MANDRIVA	<a href="#">www.mandriva.co</a>
USN-446-1: NAS vulnerabilities   Ubuntu	UBUNTU	<a href="#">www.ubuntu.com</a>
Ubuntu update for nas - Advisories - Secunia	SECUNIA	<a href="#">secunia.com</a>
Network Audio System Bugs Let Remote Users Deny Service or Execute Arbitrary Code - SecurityTracker	SECTRACK	<a href="#">www.securitytrack</a>
Debian -- Security Information -- DSA-1273-1 nas	DEBIAN	<a href="#">www.debian.org</a>
alugi.altervista.org/adv/nasbugs-adv.txt	MISC	<a href="#">alugi.altervista.or</a>
IBM X-Force Exchange	XF	<a href="#">exchange.xforce.i</a>
Webmail - OVH	VUPEN	<a href="#">www.vupen.com</a>

Network Audio System Local Privilege Escalation and Denial of Service Vulnerabilities	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>
<a href="http://www.radscan.com/nas/HISTORY">www.radscan.com/nas/HISTORY</a>	CONFIRM	<a href="http://www.radscan.com">www.radscan.com</a>
Network Audio System Multiple Vulnerabilities - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>
NAS: Multiple vulnerabilities — Gentoo Linux Documentation	GENTOO	<a href="http://security.gentoo.org">security.gentoo.org</a>
Mandriva update for nas - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>
Gentoo update for nas - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>
Debian update for nas - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>
SecurityFocus	BUGTRAQ	<a href="http://www.securityfocus.com">www.securityfocus.com</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

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

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