



CVE-2005-2903

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

Summary

CVE	CVE-2005-2903
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-09-14 20:03:00 UTC
Updated	2017-07-11 01:33:00 UTC
Description	Heap-based buffer overflow in NOD32 2.5 with nod32.002 1.033 build 1127, with active scanning enabled, allows remote at

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Eset Software	Nod32 Antivirus	2.5	All	All	All
Application	Eset Software	Nod32 Antivirus	2.5	All	All	All

References

Reference	Source	Link
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
Eset Software NOD32 Antivirus ARJ Archive Handling Remote Buffer Overflow Vulnerability	BID	www.securityfocus.com
'Secunia Research: NOD32 Anti-Virus ARJ Archive Handling Buffer' - MARC	BUGTRAQ	marc.info
About Secunia Research Flexera	MISC	secunia.com
Secunia - Advisories - NOD32 Anti-Virus ARJ Archive Handling Buffer Overflow	SECUNIA	secunia.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)