



CVE-2003-0062

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

Summary

CVE	CVE-2003-0062
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2003-02-19 05:00:00 UTC
Updated	2016-10-18 02:28:00 UTC
Description	Buffer overflow in Eset Software NOD32 for UNIX before 1.013 allows local users to execute arbitrary code via a long path

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	1.0.11	All	All	All
Application	Eset Software	Nod32 Antivirus	1.0.12	All	All	All
Application	Eset Software	Nod32 Antivirus	1.0.11	All	All	All
Application	Eset Software	Nod32 Antivirus	1.0.12	All	All	All

References

Reference	Source	Link
iDEFENSE	MISC	www.odefense.com
20030210 iDEFENSE Security Advisory 02.10.03: Buffer Overflow In NOD32 Antivirus Software for Unix	BUGTRAQ	marc.info
Eset Software NOD32 Antivirus Local Buffer Overflow Vulnerability	BID	www.securityfocus.com
ISS X-Force Database:nod32-pathname-bo(11282): NOD32 for UNIX long pathname buffer overflow	XF	www.iss.net
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](#)