



# CVE-2005-2926

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

## Summary

<b>CVE</b>	CVE-2005-2926
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2005-10-25 16:02:00 UTC
<b>Updated</b>	2019-10-09 22:48:00 UTC
<b>Description</b>	Stack-based buffer overflow in (1) backupsh and (2) authsh in SCO Openserver 5.0.7 allows local users to execute arbitrary

## Risk And Classification

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

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Sco	Openserver	All	All	All	All

## References

Reference	Source
SecurityTracker.com Archives - SCO OpenServer Buffer Overflow in authsh and backupsh Lets Local Users Gain Elevated Privileges	SECT
SCOSA-2005.40	SCO
SCO OpenServer authsh and backupsh Buffer Overflow Vulnerabilities - Secunia.com	SECU
20153	OSVE
20154	OSVE
iDefense Security Intelligence Deliverables -- Managed Security Services and Information Security Documents // iDefense Labs	IDEFI
SCO OpenServer Backupsh Local Buffer Overflow Vulnerability	BID
CVE Program record	CVE.C
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](#) 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](#)