



CVE-2004-2159

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

Summary

CVE	CVE-2004-2159
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-12-31 05:00:00 UTC
Updated	2017-07-11 01:31:00 UTC
Description	Multiple buffer overflows in XMLStarlet Command Line XML Toolkit 0.9.3 have unknown impact and attack vectors via (1) x

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xmlstarlet	Command Line Xml Toolkit	0.9.3	All	All	All
Application	Xmlstarlet	Command Line Xml Toolkit	0.9.3	All	All	All

References

Reference	Source	Link
SourceForge.net: File Release Notes and Changelog	CONFIRM	sour
10074	OSVDB	ww
IBM X-Force Exchange	XF	exch
XMLStarlet Command Line XML Toolkit Multiple Unspecified Buffer Overflow Vulnerabilities	BID	ww
XMLStarlet Buffer Overflows in Processing XML Data May Let Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	secl
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	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](#)