



CVE-2023-24671

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

Summary

CVE	CVE-2023-24671
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-16 12:15:00 UTC
Updated	2023-11-07 04:08:00 UTC
Description	VX Search v13.8 and v14.7 was discovered to contain an unquoted service path vulnerability which allows attackers to exe

Risk And Classification

Problem Types: CWE-428

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows	-	All	All	All
Application	Vxsearch	Vx Search	13.8	All	All	All
Application	Vxsearch	Vx Search	14.7	All	All	All

References

Reference	Source	Link	Tags
VX Search 13.8 Unquoted Service Path ≈ Packet Storm	MISC	packetstormsecurity.com	
Windows Privilege Escalation — Part 1 (Unquoted Service Path) by Sumit Verma Medium	MISC	medium.com	
Windows Privilege Escalation — Part 1 (Unquoted Service Path) by Sumit Verma Medium		medium.com	
CVE Program record	CVE.ORG	www.cve.org	cano
NVD vulnerability detail	NVD	nvd.nist.gov	cano

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)