



CVE-2023-21768

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

Summary

CVE	CVE-2023-21768
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-01-10 22:15:00 UTC
Updated	2023-04-27 19:15:00 UTC
Description	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 11	21h2	All	All	All
Operating System	Microsoft	Windows 11	21h2	All	All	All
Operating System	Microsoft	Windows 11	22h2	All	All	All
Operating System	Microsoft	Windows 11	22h2	All	All	All
Operating System	Microsoft	Windows Server 2022	-	All	All	All

References

Reference	Source	Link	Tags
Ancillary Function Driver (AFD) For Winsock Privilege Escalation ≈ Packet Storm	MISC	packetstormsecurity.com	
Security Update Guide - Microsoft Security Response Center	MISC	portal.msrc.microsoft.com	
Security Update Guide - Microsoft Security Response Center	MISC	msrc.microsoft.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

© [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](#)